Sammlung Schubert LV



Gruppen- und Substitutionentheorie

von

Prof. Dr. Eugen Netto

G. J. Göschensche Verlagshandlung, Leipzig

Sammlung Schubert

Sammlung mathematischer Lehrbücher.

Verzeichnis der erschienenen und projektierten Bände.

Erschienen sind bis September 1908:

Band I: **Elementare Arithmetik und Algebra** von Professor Dr. Hermann Schubert in Hamburg. Geb. M. 2.80.

Band II: **Elementare Planimetrie** von Prof. W. Pflieger in Münster i. E. Geb. M. 4.80.

Band III: **Ebene und sphärische Trigonometrie** von Dr. F. Bohnert in Hamburg. 2. Aufl. Geb. M. 2.—.

Band IV: **Elementare Stereometrie** von Dr. F Bohnert in Hamburg. Geb. M. 2.40.

Band V: **Niedere Analysis I. Teil: Kombinatorik, Wahrscheinlichkeitsrechnung, Kettenbrüche und diophantische Gleichungen** von Prof. Dr. Hermann Schubert in Hamburg. 2. Aufl. Geb. M. 3.60.

Band VI: **Algebra mit Einschluß der elementaren Zahlentheorie** von Dr. Otto Pund in Altona. Geb. M. 4.40.

Band VII: **Ebene Geometrie der Lage** von Prof. Dr. Rud. Böger in Hamburg. Geb. M. 5.—.

Band VIII: **Analytische Geometrie der Ebene** von Prof. Dr. Max Simon in Straßburg. Geb. M. 6.—.

Band IX: **Analytische Geometrie des Raumes I. Teil: Gerade, Ebene, Kugel** von Prof. Dr. Max Simon in Straßburg. Geb. M. 4.—.

Band X: **Differential- und Integralrechnung I. Teil: Differentialrechnung** von Prof. Dr. W. Franz Meyer in Königsberg. Geb. M. 9.—.

Band XI: **Differential- und Integralrechnung II. Teil: Integralrechnung** von Prof. Dr. W. Franz Meyer in Königsberg. Geb. M. 10.—.

Band XII: **Darstellende Geometrie I. Teil: Elemente der darstellenden Geometrie** von Dr. John Schröder in Hamburg. Geb. M. 5.—.

Band XIII: **Differentialgleichungen** von Prof. Dr. L. Schlesinger in Klausenburg. 2. Aufl. Geb. M. 8.—.

Band XIV: **Praxis der Gleichungen** von Prof. Dr. C. Runge in Hannover. Geb. M. 5.20.

Band XVIII: **Geschichte der Mathematik I. Teil** von Prof. Dr. S. Günther in München. Geb. M. 9.60.

Band XIX: **Wahrscheinlichkeits- und Ausgleichungsrechnung** von Dr. Norbert Herz in Wien. Geb. M. 8.—.

Band XX: **Versicherungsmathematik** von Dr. W. Großmann in Wien. Geb. M. 5.—.

Band XXIII: **Geodäsie** von Prof. Dr. A. Galle in Potsdam. Geb. M. 8.—.

Band XXV: **Analytische Geometrie des Raumes II. Teil: Die Flächen zweiten Grades** von Prof. Dr. Max Simon in Straßburg. Geb. M. 4.40.

Band XXVII: **Geometrische Transformationen I. Teil: Die projektiven Transformationen nebst ihren Anwendungen** von Prof. Dr. Karl Doehlemann in München. Geb. M. 10.—.

Band XXVIII: **Geometrische Transformationen II. Teil: Die quadratischen und höheren, birationalen Punkttransformationen** von Prof. Dr. Karl Doehlemann in München. Geb. M. 10.—.

Band XXIX: **Allgemeine Theorie der Raumkurven u. Flächen I. Teil** von Prof. Dr. Victor Kommerell in Reutlingen und Prof. Dr. Karl Kommerell in Heilbronn. Geb. M. 4.80.

Band XXX: **Elliptische Funktionen I. Teil: Theorie der elliptischen Funktionen aus analytischen Ausdrücken entwickelt** von Prof. Dr. Karl Boehm in Heidelberg. Geb. M. 8.60.

Band XXXI: **Theorie der algebraischen Funktionen und ihrer Integrale** von Oberlehrer E. Landfriedt in Straßburg. Geb. M. 8.50.

Band XXXII: **Theorie und Praxis der Reihen** von Prof. Dr. C. Runge in Hannover. Geb. M. 7.—.

Band XXXIV: **Liniengeometrie mit Anwendungen I. Teil** von Prof. Dr. Konrad Zindler in Innsbruck. Geb. M. 12.—.

Band XXXV: **Mehrdimensionale Geometrie I. Teil: Die linearen Räume** von Prof. Dr. P. H. Schoute in Groningen. Geb. M. 10.—.

Band XXXVI: **Mehrdimensionale Geometrie II. Teil: Die Polytope** von Prof. Dr. P. H. Schoute in Groningen. Geb. M. 10.—.

Band XXXVII: **Lehrbuch der Mechanik I: Kinematik** von Prof. Dr. Karl Heun in Karlsruhe. Geb. M. 8.—.

Band XXXVIII: **Angewandte Potentialtheorie in elementarer Behandlung I. Teil** von Prof. E. Grimsehl in Hamburg. Geb. M. 6.—.

Band XXXIX: **Thermodynamik I. Teil** von Prof. Dr. W. Voigt in Göttingen. Geb. M. 10.—.

Band XL: **Mathematische Optik** von Prof. Dr. J. Classen in Hamburg. Geb. M. 6.—.

Band XLI: **Theorie der Elektrizität und des Magnetismus I. Teil: Elektrostatik und Elektrokinetik** von Prof. Dr. J. Classen in Hamburg. Geb. M. 5.—.

Band XLII: **Theorie der Elektrizität und des Magnetismus II. Teil: Magnetismus und Elektromagnetismus** von Prof. Dr. J. Classen in Hamburg. Geb. M. 7.—.

Band XLIII: **Theorie der ebenen algebraischen Kurven höherer Ordnung** von Dr. Heinr. Wieleitner in Speyer. Geb. M. 10.—.

Band XLIV: **Allgemeine Theorie der Raumkurven und Flächen II. Teil** von Prof. Dr. Victor Kommerell in Reutlingen und Prof. Dr. Karl Kommerell in Heilbronn. Geb. M. 5.80.

Band XLV: **Niedere Analysis II. Teil: Funktionen, Potenzreihen, Gleichungen** von Prof. Dr. Hermann Schubert in Hamburg. Geb. M. 3.80.

Band XLVI: **Thetafunktionen und hyperelliptische Funktionen** von Oberlehrer E. Landfriedt in Straßburg. Geb. M. 4.50.

Band XLVIII: **Thermodynamik II. Teil** von Prof. Dr. W. Voigt in Göttingen. Geb. M. 10.—.

Band XLIX: **Nichteuklidische Geometrie** von Prof. Dr. Heinr. Liebmann in Leipzig. Geb. M. 6.50.

Band L: **Gewöhnliche Differentialgleichungen beliebiger Ordnung** von Dr. J. Horn, Professor an der Bergakademie zu Clausthal. Geb. M. 10.—.

Band LI: **Liniengeometrie mit Anwendungen II. Teil** von Prof. Dr. Konrad Zindler in Innsbruck. Geb. M. 8.—.

Band LII: **Theorie der geometrischen Konstruktionen** von Professor Aug. Adler in Wien. Geb. M. 9.—.

Band LIII: **Grundlehren der neueren Zahlentheorie** von Professor Dr. Paul Bachmann in Weimar. Geb. M. 6.50.

Band LIV: **Analytische Geometrie auf der Kugel** von Studienrat Prof. Dr. Rich. Heger in Dresden. Geb. M. 4.40.

Band LV: **Gruppen- u. Substitutionentheorie** von Prof. Dr. Eugen Netto in Gießen. Geb. M. 5.20.

In Vorbereitung bzw. projektiert sind:

Darstellende Geometrie von Prof. Dr. Th. Schmid in Wien.

Geschichte der Mathematik II. Teil von Prof. Dr. A. v. Braunmühl in München.

Dynamik von Prof. Dr. Karl Heun in Karlsruhe.

Technische Mechanik von Prof. Dr. Karl Heun in Karlsruhe.

Allgemeine Funktionentheorie von Dr. Paul Epstein in Straßburg.

Räumliche projektive Geometrie.

Elliptische Funktionen II. Teil von Dr. Karl Boehm in Heidelberg.

Allgemeine Formen- und Invariantentheorie von Prof. Dr. W. Franz Meyer in Königsberg.

Angewandte Potentialtheorie in elementarer Behandlung II. Teil von Prof. E. Grimsehl in Hamburg.

Liniengeometrie III. Teil von Prof. Dr. Konrad Zindler in Innsbruck.

Elektromagnetische Lichttheorie von Prof. Dr. J. Classen in Hamburg.

Theorie der Flächen dritter Ordnung.

Mathematische Potentialtheorie von Prof. Dr. A. Wangerin in Halle.

Elastizitäts- und Festigkeitslehre im Bauwesen von Dr.-Ing. H. Reißner in Berlin.

Elastizitäts- und Festigkeitslehre im Maschinenbau von Dr. Rudolf Wagner in Stettin.

Graphisches Rechnen von Prof. Aug. Adler in Wien.

Partielle Differentialgleichungen von Professor J. Horn in Clausthal.

Vektorenanalyse.

Spezielle algebraische und transzendente ebene Kurven von Dr. Heinr. Wieleitner in Speyer.

Sphärische Astronomie von Dr. von Flotow in Charlottenburg.

Grundlehren der geographischen Ortsbestimmung von Dr. K. Graff in Hamburg.

Theoretische Astronomie von Dr. Gust. Witt in Berlin.

Astrophysik.

Grundlagen der theoretischen Chemie von Dr. Franz Wenzel in Wien.

Sammlung Schubert LV

Gruppen- und Substitutionentheorie

von

Dr. Eugen Netto
O. Professor an der Universität zu Gießen



Leipzig
G. J. Göschen'sche Verlagshandlung
1908

Spamersche Buchdruckerei in Leipzig

Vorwort.

Dem Plane dieser Sammlung entsprechend hat sich der Verfasser die Aufgabe gestellt, im vorliegenden Buche eine möglichst elementar gehaltene Einführung in die Gruppen- und Substitutionentheorie zu geben. An einigen Stellen, besonders im 7. Kapitel, war dies mit großen Schwierigkeiten verbunden; aber die Wichtigkeit des Gebotenen überwog formale Bedenken. Daß ein so vorzügliches Werk wie die „Theory of groups of finite order“ von W. Burnside nicht ohne Einfluß auf Anordnung und Stoff des hier Gebotenen war, bedarf keiner Rechtfertigung. — Die Anwendungen der behandelten Theorie, besonders bei algebraischen Fragen, zu geben, lag nicht in der Absicht des Verfassers.

E. Netto.

Inhaltsverzeichnis.

1. Kapitel.

Seite

Grundbegriffe der Gruppentheorie . . . 1—20

§ 1. Definition von Gruppen. — Operator 1
§ 2. Beispiele 2
§ 3. Beispiele. Endliche und unendliche Gruppen . . . 3
§ 4. Folgerungen für endliche Gruppen 4
§ 5. Permutationen. — Substitutionen 5
§ 6. Substitutionengruppen 6
§ 7. Zyklendarstellung 8
§ 8. Potenz. — Ordnung 9
§ 9. Transpositionendarstellung 10
§ 10. Inversionen. — Klassen 11
§ 11. Folgerungen. Symmetrische und alternierende Gruppe 12
§ 12. Weitere Untersuchungen 15
§ 13. Abstrakte Gruppen. Ordnung. Einheitsoperator . . 15
§ 14. Reziproke 17
§ 15. Zerlegung eines Operators 18

2. Kapitel.

Das Cayleysche Quadrat . . . . . . 20—33

§ 16. Das Cayleysche Quadrat 20
§ 17. Gruppen niedrigster Ordnungen 23
§ 18. Reguläre Substitutionengruppen 27
§ 19. Gruppen, bestimmt durch einen und durch zwei Operatoren 29
§ 20. Widerspruchsvolle Bestimmung 31
§ 21. Unendliche Gruppe 32

3. Kapitel.

Teiler einer Gruppe. Isomorphismus . . 34—46

§ 22. Bezeichnungen 34
§ 23. Teiler und ihre Ordnung 35
§ 24. Nebenkomplexe 36
§ 25. Anwendung auf Substitutionengruppen 38
§ 26. Alternierende Gruppen; Index 2 39
§ 27. Isomorphismus, einstufig 40
§ 28. Gruppe sich selbst isomorph 42
§ 29. Isomorphismus, mehrstufig 43
§ 30. Isomorphes Entsprechen von Teilern 44

4. Kapitel.

Seite

Transformation und Vertauschbarkeit . . 47–64

§ 31. Transformation 47
§ 32. Anwendung auf Substitutionen 48
§ 33. Transformierte haben gleiche Ordnung 49
§ 34. Vertauschbarkeit von Operatoren 50
§ 35. Vertauschbare oder Abelsche Gruppen 52
§ 36. Vertauschbarkeit von Operator und Gruppe 52
§ 37. Zwischengruppe. Zusammengesetzte und einfache Gruppe 54
§ 38. Transformationskomplex. Konjugierte Gruppen . . 55
§ 39. Anwendung auf Gruppen der Ordnung p^α 56
§ 40. Vertauschbarkeit von Gruppen 56
§ 41. Erste Anwendung 58
§ 42. Zweite Anwendung 59
§ 43. Faktorgruppe und Isomorphismus 60
§ 44. Beispiel 61
§ 45. Teiler der selbstkonjugierten Operatoren 61
§ 46. Faktorgruppe bei Transformierten 63

5. Kapitel.

Zusammengesetzte Gruppen 64--82

§ 47. Elementare Eigenschaften 64
§ 48. Selbstkonjugierter Maximalteiler 65
§ 49. Hilfssatz 65
§ 50. Anwendung 67
§ 51. Kompositionsreihe 67
§ 52. Verschiedene für eine Gruppe 68
§ 53. Kompositionsreihe mit vorgeschriebenem Teiler . . 69
§ 54. Kompositionsreihe eines Teilers 70
§ 55. Hauptreihe 71
§ 56. Verschiedene für eine Gruppe 72
§ 57. Verhältnis der Kompositions- zur Hauptreihe . . . 72
§ 58. Vorletzte Gruppe der Hauptreihe 74
§ 59. Gruppen der Ordnung p^α 76
§ 60. Eigenschaft ihrer Teiler der Ordnung $p^{\alpha-1}$ 77
§ 61. Vorletztes Glied der Hauptreihe von der Ordnung p 78
§ 62. Anzahl der Teiler der Ordnung p^ϱ 79
§ 63. Anwendung auf Gruppen der Ordnung p^2 80
§ 64. Die alternierende Gruppe ist einfach 81

6. Kapitel.

Abelsche Gruppen . . . . 82—98

§ 65. Elementare Eigenschaften 82
§ 66. Zerlegung; Ordnung p^α 83

Seite
§ 67. Basis der Gruppe 84
§ 68. Invarianten 86
§ 69. Isomorphismus 89
§ 70. Allgemeine Gruppen 90
§ 71. Gruppen der Ordnung 8 91
§ 72. Wahl der Basis 94
§ 73. Hamiltonsche Gruppen 94
§ 74. Ihre Zerlegung 96
§ 75. Gruppen der Ordnung p^α 97

7. Kapitel.

Sätze von Sylow und von Frobenius . . 98—115
§ 76. Aufstellung des Problems 98
§ 77. Lösung für Abelsche Gruppen 99
§ 78. Hilfssatz; Doppelmodul 99
§ 79. Sylows erster Satz 101
§ 80. Sylows zweiter Satz 103
§ 81. Sylows dritter Satz 103
§ 82. Frobenius erster Satz 105
§ 83. Folgerungen 109
§ 84. Frobenius zweiter Satz 110
§ 85. Gruppen der Ordnung $p \cdot q$ 113

8. Kapitel.

Auflösbare Gruppen . . . . . . 115—123
§ 86. Definition 115
§ 87. Kriterium von Galois 116
§ 88. Kriterium von Jordan 117
§ 89. Teiler auflösbarer Gruppen 118
§ 90. Besondere Fälle 119
§ 91. Sylowscher Satz 120
§ 92. Frobeniusscher Satz 121
§ 93. Folgerung 122
§ 94. Erweiterter Satz 122
§ 95. Weitere Theoreme 122

9. Kapitel.

Substitutionengruppen. — Transitivität . 123—142
§ 96. Definition 123
§ 97. Ordnung transitiver Gruppen 125
§ 98. Transitivität von Untergruppen 126
§ 99. Vorkommen einer Zirkularsubstitution dritter Ordnung 127
§ 100. Substitutionen geringsten Grades 127
§ 101. Substitutionen höchsten Grades 129
§ 102. Bestimmung einer Gruppe durch sie 130
§ 103. Metazyklische Gruppen 132

Seite

§ 104. k-fach transitive Gruppe als Teiler einer $(k+1)$-fach transitiven 135
§ 105. Beispiel 137
§ 106. Intransitive Gruppen 139
§ 107. Vertauschbarkeit transitiver Gruppen 140
§ 108. Abelsche transitive Gruppen 141
§ 109. Reguläre transitive Gruppen 141

10. Kapitel.

Substitutionengruppen. — Primitivität . 142—156

§ 110. Definition 142
§ 111. Theoreme 143
§ 112. Verschiedene Systemeinteilung 144
§ 113. Maximalordnungen 144
§ 114. Transitiver Teiler primitiver Gruppen 145
§ 115. Teiler, der ein Element nicht umsetzt 146
§ 116. Reguläre transitive Gruppen 147
§ 117. Primitive Gruppen mit Transpositionen 148
§ 118. Auflösbare primitive Gruppen 148
§ 119. Darstellung abstrakter Gruppen als Substitutionengruppen 149
§ 120. Darstellung durch primitive Gruppen 150
§ 121. Folgerungen 151
§ 122. Allgemeines Problem 152
§ 123. Primitive Gruppen niedrigster Grade 154

11. Kapitel.

Substitutionengruppen. — Gruppen höchster Ordnungen bei gegebenem Grade . . . . . 156—163

§ 124. Gruppen, deren Ordnung $>(n-1)!$ beim Grade n . 156
§ 125. Gruppen, deren Ordnung $=(n-1)!$ 158
§ 126. Gruppen, deren Ordnung $=120$ beim Grade 6 . . . 160
§ 127. Gruppen, deren Ordnung $>(n-k)!$ 163

12. Kapitel.

Analytische Darstellung der Substitutionen. Die lineare Gruppe . . . . 164—175

§ 128. Darstellung durch Funktionen für die Indizes . . . 164
§ 129. Arithmetische Gruppe 165
§ 130. Die lineare Gruppe 166
§ 131. Ihre Ordnung 168
§ 132. Teiler mit der Determinante 1 169
§ 133. Reduktion der Darstellung 169
§ 134. Auflösbare Gruppen vom Primzahlgrad p 173
§ 135. Vom Grade p^λ 174

---

1. Kapitel.

Grundbegriffe der Gruppentheorie.

§ 1. Eine Reihe von Elementen $a, b, c, d, e, \ldots$ möge folgende drei Eigenschaften besitzen:

I. Die Verknüpfung von zwei beliebigen Elementen a und b der Elementenreihe in gegebener Folge bestimmt eindeutig ein drittes der Reihe. Diese Verknüpfung nennen wir Komposition und die Operation selbst: komponieren. Man kann zwei Elemente a und b je nach ihrer Anordnung auf zwei Arten komponieren; die Bezeichnung der Komposition von a und b ist je nach der Ordnung der Elemente $a \cdot b$ oder $b \cdot a$, also mit der Produktbezeichnung der Algebra identisch; der Punkt, das Multiplikationszeichen, darf auch unterdrückt werden. Ein Element kann mit sich selbst komponiert werden.

II. Aus jeder der beiden Gleichungen

$$ac = bc \quad \text{und} \quad ca = cb \tag{1}$$

folgt die Gleichheit $a = b$.

III. Für die Komposition von drei Elementen a, b, c gilt das assoziative Gesetz

$$(ab) \cdot c = a \cdot (bc) \; ; \tag{2}$$

anders ausgedrückt: wenn $ab = d$ und $bc = e$, so ist $dc = ae$.

Sind diese drei Annahmen verwirklicht, so sagt man: die Elemente $a, b, c, d, e, \ldots$ bilden eine Gruppe.

Das bei gewöhnlicher Multiplikation bestehende kommutative Gesetz $ab = ba$ gilt für Gruppen im allgemeinen nicht; darin liegt der Unterschied zwischen Komposition und Multiplikation und die erweiternde Bedeutung der ersten. Wir werden gleichwohl, sobald Verwechselungen

nicht zu befürchten sind, die algebraischen Ausdrücke Multiplikation, Produkt, Faktor auch in der Gruppentheorie verwenden.

Bei einem Produkt ab heiße a die linke Komponente oder der linke Faktor, b die rechte Komponente oder der rechte Faktor; aus a das Produkt ab (oder ba) herleiten heiße „a mit b rechtsseitig (bzw. linksseitig) multiplizieren".

Die Elemente $a, b, c, d, e, \ldots$ können irgendwelche Dinge sein, von denen nur vorausgesetzt wird, daß sie voneinander verschieden und unterscheidbar sind. Wir können aber unter den Elementen auch Operationen verstehen, die an gegebenen Objekten vorgenommen werden. Für beide Möglichkeiten bietet der folgende Paragraph Beispiele dar. Weil bei der besonders wichtigen Verwendung der Gruppentheorie auf Permutationen die Bezeichnung „Element" für die zu permutierenden Gegenstände gebraucht wird, so wollen wir bei unseren allgemeinen Betrachtungen für die $a, b, c, \ldots$ durchgängig die Bezeichnung „Operatoren" verwenden, wie dies von englischen Autoren eingeführt ist.

Unabhängig von der Geltung der drei gemachten Voraussetzungen über die Elemente oder Operatoren nennen wir eine gegebene Gesamtheit von Elementen oder Operatoren einen Komplex oder eine Komplexion.

§ 2. Gruppenbildungen kommen in der Mathematik recht häufig vor.

Alle ganzen und auch schon alle positiven ganzen Zahlen bilden bei Verwendung der Addition als Kompositionsgesetz eine Gruppe; die ungeraden Zahlen allein bilden hierbei nur einen Komplex, keine Gruppe; die geraden Zahlen bilden auch hier für sich eine Gruppe. — Wählt man die Multiplikation als Kompositionsvorschrift bei den ganzen Zahlen, so tritt gleichfalls nur ein Komplex auf; denn die Annahme II, § 1 ist verletzt, da aus $a \cdot 0 = b \cdot 0$ nicht $a = b$ gefolgert werden kann. Dagegen bilden hier die ganzen und auch die geraden Zahlen mit Ausschluß der Null eine Gruppe. — Bei der Verwendung der Division als Kompositionsvorschrift bilden die rationalen Zahlen mit Ausschluß der Null eine Gruppe. — Das Potenzieren kann nicht als Kompositionsvorschrift benutzt

werden, da wegen der im allgemeinen geltenden Beziehung

$$(a^b)^c \neq a^{(b^c)}$$

die Bedingung III verletzt wird.

Auch geometrische Betrachtungen führen zu Gruppenbildungen. Ist z. B. einer Kugel einer der fünf regulären Körper: Tetraeder, Hexaeder, Oktaeder, Dodekaeder, Ikosaeder einbeschrieben, etwa ein Tetraeder, so kann jede Bewegung der Kugelfläche in sich, die das Tetraeder in sich selbst überführt, als Operator einer Gruppe aufgefaßt werden, gleichgültig, ob hierdurch die Ecken ihre früheren Plätze einnehmen oder sie untereinander vertauschen. Eine speziellere Gruppe wird dabei erhalten, wenn man nur Drehungen, d. h. solche Bewegungen benutzt, bei denen eine Achse fest bleibt, oder wenn man jede Ecke auf ihren ursprünglichen Platz zurückführt.

§ 3. In den soeben besprochenen arithmetischen und geometrischen Beispielen trat eine unendliche Anzahl von Operatoren auf. Es lassen sich aber leicht auch Gruppen mit einer endlichen Operatorenzahl herleiten.

Betrachten wir, wie es in der Zahlentheorie üblich ist, statt der ganzen Zahlen selbst nur ihre Reste bei der Division durch eine, für die gesamte Betrachtung feste ganze Zahl, den Modul, und rechnen wir alle Zahlen, die bei der Division durch den Modul den gleichen Rest lassen, zu einer Klasse, so können wir diese Klassen, deren Anzahl der Größe des Moduls gleichkommt, als Operatoren ansehen.

Dabei hat für einen beliebigen Modul n bei der Addition als Kompositionsvorschrift der Komplex der durch die n Restklassen $0, 1, 2, \ldots (n-1)$ gegebenen Operatoren die Gruppeneigenschaft.

Bei der Verwendung der Multiplikation auf diese Klassen ist das nicht mehr ohne weiteres so. Nehmen wir z. B. $n = 8$, so kann aus der Kongruenz

$$a \cdot 4 \equiv b \cdot 4 \pmod{8}$$

nicht geschlossen werden $a \equiv b \pmod{8}$, wie man z. B. aus $a = 1$, $b = 3$ ersieht. Dagegen entsteht auch hier eine Gruppe, falls der Modul eine Primzahl ist.

Je nach der endlichen oder der unendlichen Anzahl ihrer Operatoren heißt die Gruppe eine endliche oder eine unendliche. Die Anzahl der Operatoren einer Gruppe heißt ihre Ordnung. Wir beschäftigen uns im folgenden fast ausschließlich mit endlichen Gruppen.

§ 4. Bei endlichen Gruppen lassen sich aus den Forderungen I und II des § 1 einige wichtige Schlüsse ziehen.

Bedeutet a einen beliebigen festen Operator der Gruppe und x einen unbestimmten Operator derselben Gruppe, der der Reihe nach alle Operatoren $x_1, x_2, x_3, \ldots, x_n$ der Gruppe von der Ordnung n durchläuft, so gibt es nach I, § 1 Operatoren $y_1, y_2, \ldots, y_n$ der Gruppe, die bzw. die Gleichungen

$$y_1 = a\,x_1\,, \quad y_2 = a\,x_2\,, \quad y_3 = a\,x_3\,, \quad \ldots, \quad y_n = a\,x_n$$

befriedigen. Wie die x_λ, so sind hierin auch die y_λ untereinander verschieden, da aus $a\,x_\alpha = a\,x_\beta$ nach II, § 1 folgen würde $x_\alpha = x_\beta$. Mit den x_λ durchläuft also $y_\lambda = a\,x_\lambda$ alle Operatoren der Gruppe und wird jedem ein- und nur einmal gleich. Daher gibt es stets einen und auch nur einen Operator der Gruppe, der die Gleichung mit der Unbekannten x befriedigt

$$a\,x = b\,.$$

In entsprechender Weise läßt sich zeigen, daß in endlichen Gruppen die Gleichung mit der unbekannten linken Komponente

$$x\,a = b$$

für jedes a und jedes b eine und nur eine Lösung x hat.

Bei unendlichen Gruppen versagen die verwendeten Schlüsse, und die Resultate gelten nicht mehr. Das erkennt man einfach schon aus folgendem Beispiele. Die Operatoren einer Gruppe seien sämtliche Potenzen mit positiven und verschwindendem Exponenten

$$1,\ a\,,\ a^2,\ a^3,\ a^4,\ \ldots,\ a^n,\ \ldots$$

einer Größe a, die a weder gleich Null noch irgend eine Einheitswurzel sein soll. Als Kompositionsvorschrift gelte die Multiplikation. Dann bilden diese Potenzen eine Gruppe, denn es sind die Bestimmungen I, II, III in § 1

in Kraft. Die Anzahl der Operatoren dieser Gruppe ist unendlich groß; denn aus einer Gleichung $a^k = a^l$ würde folgen, daß a gleich Null oder gleich einer Einheitswurzel ist. Wie man sieht, haben aber die Gleichungen

$$a^2 x = a\,,\quad x a^2 = a\,,\quad a^{k+l} x = a^k\,,\quad \ldots \qquad (k\,,\, l > 0)$$

keine Lösungen für die Unbekannte x innerhalb der Gruppe.

§ 5. Die Permutationen einer endlichen Anzahl gegebener Elemente bilden eins der wichtigsten Beispiele für endliche Gruppen. Sind n untereinander verschiedene Elemente $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ vorgelegt, so bezeichnet man jede andere Reihenfolge derselben Elemente

$$\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, \ldots, \alpha_{i_n},$$

wo die $i_1, i_2, \ldots, i_n$ bis auf ihre Anordnung mit den Zahlenindizes $1, 2, \ldots, n$ übereinstimmen, als eine Permutation der ursprünglichen Elementenfolge. Die Operation des Überganges von einer ersten zu einer zweiten Anordnung nennt man eine Substitution. Man bezeichnet sie durch das Symbol

$$(3)\quad s_i = \begin{pmatrix} \alpha_1, & \alpha_2, & \alpha_3, & \ldots, & \alpha_n \\ \alpha_{i_1}, & \alpha_{i_2}, & \alpha_{i_3}, & \ldots, & \alpha_{i_n} \end{pmatrix} = \begin{pmatrix} \alpha_k \\ \alpha_{i_k} \end{pmatrix} \quad (k = 1, 2, 3, \ldots, n)$$

oder einfacher durch eins der Symbole, die nur die Indizes der Elemente angeben

$$(3^*)\qquad s_i = \begin{pmatrix} 1, & 2, & 3, & \ldots, & n \\ i_1, & i_2, & i_3, & \ldots, & i_n \end{pmatrix} = \begin{pmatrix} \varrho \\ i_\varrho \end{pmatrix} = \varrho\,, i_\varrho|\,,$$
$$(\varrho = 1, 2, 3, \ldots, n)\,.$$

Als Substitution betrachten wir auch den Fall, daß man kein Element umstellt, so daß also jedes $k = i_k$ ist; hierfür gehen (3) und (3*) über in die Form

$$(4)\qquad \begin{pmatrix} 1, & 2, & 3, & \ldots, & n \\ 1, & 2, & 3, & \ldots, & n \end{pmatrix} = \begin{pmatrix} \varrho \\ \varrho \end{pmatrix} = |\varrho\,, \varrho| = 1\,.$$

Wir nennen das die identische oder die Einheitssubstitution.

Die erste Zeile der eingeführten Klammersymbole (3),

(3*), (4) kann ganz beliebig angeordnet werden. So kann man statt (3*) auch schreiben

$$s_i = \begin{pmatrix} 3, & 1, & 5, & 4, & \dots \\ i_3, & i_1, & i_5, & i_4, & \dots \end{pmatrix} = \dots = \begin{pmatrix} n, & n-1, & \dots, & 2, & 1 \\ i_n, & i_{n-1}, & \dots, & i_2, & i_1 \end{pmatrix} = \dots$$

Die Anzahl der Substitutionen unter n Elementen ist der der Permutationen gleich, also $n!$

Wir wollen diese Substitutionen von n Elementen zu Operatoren einer Gruppe machen. Dazu definieren wir die Komposition zweier Substitutionen s_i und s_k als die Substitution, die entsteht, wenn man auf die ursprünglich gegebene Anordnung $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$ der Elemente zuerst s_i und auf die dadurch hervorgerufene neue Anordnung die Substitution s_k anwendet. Für die Gesamtheit der $n!$ Substitutionen ist dabei I, § 1 erfüllt.

Das „Produkt“ der Operatoren s_i, s_k ist leicht als Substitution darzustellen. Hat man nämlich als „Faktoren“ die beiden Substitutionen

(5) $$s_i = |\varrho, i_\varrho|, \quad s_k = |\varrho, k_\varrho|,$$

so wird, wie man sofort erkennt,

(6) $$s_i s_k = |\varrho, i_\varrho| \cdot |\varrho, k_\varrho| = |\varrho, i_\varrho| \cdot |i_\varrho, k_{i_\varrho}| = |\varrho, k_{i_\varrho}|;$$

denn offenbar sagt $|i_\varrho, k_{i_\varrho}|$ dasselbe aus wie $|\varrho, k_\varrho|$, so daß der zweite Ausdruck in (6) dem dritten gleich wird.

Ebenso erhält man für die umgekehrte Folge der Faktoren das Resultat

(6*) $$s_k s_i = |\varrho, i_{k_\varrho}|.$$

Die Vergleichung von (6) und (6*) zeigt, daß das kommutative Gesetz nicht zu gelten braucht; denn es wird im allgemeinen i_{k_ϱ} von k_{i_ϱ} verschieden sein.

Ferner folgt das assoziative Gesetz aus den Gleichungen

$$(s_i s_k) s_l = |\varrho, k_{i_\varrho}| \cdot |\varrho, l_\varrho| = |\varrho, l_{k_{i_\varrho}}|,$$

$$s_i (s_k s_l) = |\varrho, i_\varrho| \cdot |\varrho, l_{k_\varrho}| = |\varrho, l_{k_{i_\varrho}}|;$$

somit ist auch die Forderung III, § 1 erfüllt.

§ 6. Um auch über II, § 1 ins klare zu kommen, verfahren wir so:

Mit jeder Substitution s_i ist eine andere s'_i verknüpft, derart, daß

$$s_i = |\varrho, i_\varrho|, \quad s'_i = |i_\varrho, \varrho|$$

ist. Die Komposition beider ergibt rechtsseitig und linksseitig in gleicher Weise

$$s_i s'_i = |\varrho, \varrho| = 1, \quad s'_i s_i = |i_\varrho, i_\varrho| = 1.$$

Das Produkt aus s_i, s'_i oder aus s'_i, s_i liefert also die oben bereits eingeführte identische Substitution, d. h. die, die überhaupt kein Element umstellt. Wegen dieser Eigenschaft nennen wir jede der beiden s_i und s'_i die Reziproke der anderen und schreiben

$$s'_i = s_i^{-1} \quad \text{und} \quad s_i = (s'_i)^{-1}.$$

Ist

$$s = \begin{pmatrix} a_k \\ a_{i_k} \end{pmatrix},$$

so wird

$$s^{-1} = \begin{pmatrix} a_{i_k} \\ a_k \end{pmatrix}.$$

Die Reziproke der Reziproken ist die ursprüngliche Substitution.

Jetzt können wir leicht auch II, § 1 bei dem Komplexe aller $n!$ Substitutionen als erfüllt nachweisen. Ist nämlich eine der beiden Gleichungen

$$s_i s_k = s_i s_l \quad \text{oder} \quad s_k s_i = s_l s_i$$

befriedigt, so folgt aus der ersten durch linksseitige Multiplikation mit s'_i

$$s_k = s_i^{-1}(s_i s_k) = s_i^{-1}(s_i s_l) = s_l,$$

und aus der zweiten Gleichung durch rechtsseitige Multiplikation mit s'_i

$$s_k = (s_k s_i) s_i^{-1} = (s_l s_i) s_i^{-1} = s_l.$$

Folglich bildet die Gesamtheit der $n!$ Substitutionen von n Elementen eine Gruppe. Sie heißt die symmetrische Substitutionengruppe. Ihre Ordnung ist $n!$.

Greift man aus dieser Gruppe r beliebige Substitutionen $s_\alpha, s_\beta, s_\gamma, \ldots$ heraus, so gelten für ihren Komplex

noch immer die Forderungen II und III, § 1; dagegen gilt I nicht notwendig. Sind aber die Substitutionen so gewählt, daß mit s_α und s_β auch $s_\alpha \cdot s_\beta$ dem Komplexe angehört, wie auch immer s_α, s_β aus dem Komplexe gewählt sind, so geht der Komplex in eine Gruppe der Ordnung r über. Eine jede solche Gruppe soll als Substitutionengruppe bezeichnet werden. Die Anzahl der durch die Substitutionen versetzten Elemente einer Substitutionengruppe heißt ihr Grad.

Die Aufstellung aller möglichen Substitutionengruppen des Grades n ist ein äußerst wichtiges und ebenso schwieriges Problem, von dessen Lösung wir noch weit entfernt sind. Mechanisch würde die Frage so behandelt werden können, daß man r beliebige Substitutionen ($r = 2, 3, 4, \ldots, n!$) auf alle Arten auswählt und ihren Komplex rechnerisch auf die Gruppeneigenschaft I hin untersucht.

§ 7. Die Bezeichnung der Substitutionen läßt sich bequemer gestalten.

Gehen wir in (3) oder (3*) von einem Elemente a der oberen Zeile aus, so wird dies durch die Substitution s_i in ein Element b der unteren Zeile übergeführt; dies b der ersten Zeile dann ebenso in ein c der unteren, weiter in gleicher Art dies in d, und weiter, bis endlich ein so erhaltenes Element g wieder in ein früheres umgewandelt wird. In ein späteres als das Ausgangselement a kann g nicht verwandelt werden; denn folgte dem g z. B. das c, so stände dies mit der früheren Folge $b\,c$ im Widerspruch. Also folgt a auf g. Die auf diese Art erhaltenen Elemente schließen wir in eine runde Klammer ein, nennen sie einen Zykel und deuten also das Symbol

$$(a\,b\,c \ldots f\,g)$$

so, daß jedes Element $a, b, c, \ldots, f, g, a$ durch das folgende ersetzt wird. Man kann den Zykel mit einem beliebigen seiner Elemente beginnen, muß nur die gleiche Folge der Elemente innehalten und auf das letzte Element das erste folgen lassen. So haben die Zykel derselben fünf Elemente a, b, c, d, e

$$(a\,b\,c\,d\,e),\ (b\,c\,d\,e\,a),\ (c\,d\,e\,a\,b),\ (d\,e\,a\,b\,c),\ (e\,a\,b\,c\,d)$$

sämtlich die gleiche Bedeutung, nämlich $\begin{pmatrix} a\,b\,c\,d\,e \\ b\,c\,d\,e\,a \end{pmatrix}$.

Sind alle gegebenen Elemente, die die Substitution enthält, durch den einen Zykel erschöpft, so heißt die Substitution eine zyklische. Gibt es außer den in sie eingehenden noch andere Elemente, dann gibt eins von diesen neuen die Veranlassung zur Bildung eines zweiten Zykels usf. So verteilen sich alle Elemente in einzelne Zykel. Steht dabei ein Element allein in einem Zykel, so stellt die Substitution dieses Element nicht um; und umgekehrt. Solche Elemente können dann einfach fortgelassen werden, wenn es nicht darauf ankommt, die Elemente der Substitution sämtlich ersichtlich zu machen.

Jedes Element einer Substitution tritt bei dieser Schreibweise nur in einem ihrer Zykel und nur einmal auf.

Die Darstellung einer Substitution geschieht nun so, daß alle ihre Zykel in beliebiger Folge hintereinander geschrieben werden; so ist z. B.

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 \\ 3 & 9 & 7 & 4 & 8 & 2 & 1 & 5 & 0 & 6 \end{pmatrix}$$

$$= (137)\,(2906)\,(4)\,(58) = (9062)\,(371)\,(85)$$

$$= (85)\,(713)\,(0629) = \ldots$$

§ 8. Die Kompositionsbildung ist auch bei dieser Darstellung einfach. Soll $s \cdot t$ gebildet werden, und hat s in einem Zykel die Folge $a\,b$, so sucht man in t das Element auf, das auf b folgt. Heißt dies c, dann kommt in $s \cdot t$ die Folge $a\,c$ vor usw. So liefert das obige s und die Substitution

$$t = (1435)\,(026)\,(78)\,(9)$$

je nach der Anordnung der Faktoren die Produkte

$$s\,t = (157438)\,(29)\,; \quad t\,s = (147538)\,(90)\,.$$

Auch hier ist das kommutative Gesetz außer Kraft, wie das Beispiel zeigt.

Die Produktbildung leitet zur Potenzbildung hin. Hat die Substitution

	s die Elementenfolgen		$a_1\,a_2\,a_3\,a_4\,a_5\,a_6\,a_7\,\ldots,$
so hat	s^2 ,,	,,	$a_1\,a_3\,a_5\,a_7\,\ldots,\ a_2\,a_4\,a_6\,\ldots,$
,, ,,	s^3 ,,	,,	$a_1\,a_4\,a_7\ldots,\ a_2\,a_5\ldots,\ a_3\,a_6\ldots$

Hiernach wird die $\varkappa$te Potenz einer zyklischen Substitution von $\varkappa$ Elementen gleich der identischen Substitution 1, z. B.

$$(12)^2 = 1\,; \quad (a\,b\,c)^3 = 1\,; \quad (\alpha_1\,\alpha_2\,\alpha_3\,\alpha_4)^4 = 1\,; \quad \ldots$$

Die Zahl $\varkappa$ heißt dabei die Ordnung der zyklischen Substitution.

Allgemeiner wird die $\varkappa$te Potenz einer beliebigen Substitution gleich 1, wenn $\varkappa$ ein gemeinsames Vielfaches der Ordnungszahlen all ihrer Zyklen ist. Der niedrigste Exponent $\varkappa_0$, der eine Potenz der Substitution zu 1 macht, ist das kleinste gemeinsame Vielfache der Ordnungen ihrer Zyklen; dieses $\varkappa_0$ heißt die Ordnung der Substitution.

§ 9. Die Zyklen aus zwei Elementen $(a\,b)$ sind nach der Einheit die einfachsten aller Substitutionen. Sie heißen Transpositionen. Ihre Wirkung besteht in der Umsetzung der beiden Elemente der Klammer. Jede Transposition ist ihrer Reziproken gleich. Es gilt der wichtige Satz: Jede Substitution läßt sich als ein Produkt von Transpositionen darstellen. Es ist nämlich:

$$(a\,b\,c\,\ldots\,d)\,(f\,g\,h\,\ldots\,k)\ldots$$
$$= (a\,b)\,(a\,c)\ldots(a\,d)\cdot(f\,g)\,(f\,h)\ldots(f\,k)\ldots$$

Man sieht aus $(a\,b)\,(a\,b) = 1$, daß bei dieser Schreibweise die Elemente mehrfach auftreten können.

Für die Darstellung der Substitutionen durch Transpositionen reicht es aus, in dem Produkte nur Transpositionen zu verwenden, die ein bestimmt vorgeschriebenes Element, etwa a enthalten; denn es ist ja

$$(b\,c) = (a\,b)\,(a\,c)\,(a\,b)\,.$$

Es sind also bei Substitutionen von n Elementen nur die $n-1$ Transpositionen nötig, die ein bestimmtes Element enthalten, um alle Substitutionen als Produkte von Transpositionen zu liefern.

Schon hieraus erkennt man, daß die Darstellung einer gegebenen Substitution aus Transpositionen auf unendlich viele Arten erfolgen kann. Bei allen diesen Darstellungen tritt als invariante Eigenschaft heraus, daß die Anzahl der Faktoren stets gerade oder stets ungerade ist,

d. h. modulo 2 denselben Rest gibt. Das wollen wir unter Einführung eines neuen Begriffes beweisen. Zunächst schließen wir aber aus dem Besprochenen, daß eine Substitutionengruppe der n Elemente $a, b, c, \ldots, f, g$, die alle oder auch nur die $(n-1)$ Transpositionen

$$(a b), (a c), \ldots, (a f), (a g)$$

enthält, die symmetrische Gruppe der Elemente ist.

§ 10. Der neu einzuführende Begriff ist der der Inversion. Liegt eine Reihe von Elementen vor, bei denen eine Unterscheidung darüber möglich ist, welches von je zweien das frühere und welches das spätere ist (wie z. B. bei Zahlen, die ihrer numerischen, oder bei Buchstaben, die ihrer alphabetischen Ordnung nach gegeben sind), so sagen wir: zwei Elemente einer Komplexion bilden eine Inversion, wenn das spätere der beiden Elemente dem früheren voraufgeht, gleichgültig, ob beide unmittelbar aufeinander folgen oder nicht. So liefern in der Zahlenkomplexion 317249685 die Paare 72; 74; 76; 75 je eine Inversion, 79; 78 dagegen keine. Ähnlich in $d f a c h g b$, wo $d a$; $d c$; $d b$ Inversionen bilden, $d f$; $d g$; $d h$ dagegen nicht. Die hier benutzte Zahlenkomplexion 317249685 hat im ganzen elf, die Buchstabenkomplexion $d f a c h g b$ hat zehn Inversionen. Diesen Begriff der Inversion verwenden wir zum Beweise des angeführten Satzes.

Wir unterscheiden unter Berücksichtigung der Inversionenanzahl zwei Klassen von Komplexionen: zur ersten Klasse rechnen wir die Komplexionen, bei denen die Gesamtzahl der auftretenden Inversionen gerade; zur zweiten Klasse die, bei denen diese Gesamtzahl ungerade ist. Somit gehört die obige Buchstabenkomplexion zur ersten, die Zahlenkomplexion dagegen zur zweiten Klasse.

Wendet man auf eine Komplexion eine Transposition an, so ändert sich die Klasse, zu der sie gehört. Der Satz ist ohne weiteres ersichtlich, wenn die zu transponierenden Elemente der Komplexion unmittelbar aufeinander folgen, wie z. B. 7 und 2 bei 312749685 und 317249685. Wir nehmen nun an, der Satz sei schon für die Transposition zweier Elemente bewiesen, zwischen denen höchstens ν andere stehen, und zeigen auch seine Richtigkeit für Elemente mit $(\nu+1)$ Zwischengliedern. Damit

ist er dann allgemein durch den Schluß von ν auf $(\nu + 1)$ bewiesen. Wir nehmen, das reicht völlig aus, etwa $\nu = 3$ und zeigen die Richtigkeit der Behauptung an (78) bei den Komplexionen

$$317249685 \quad \text{und} \quad 318249675 .$$

Die vorgenommene Transposition (78) läßt sich durch drei andere aufeinanderfolgende, deren Elemente näher beieinander stehen,

$$(28),\ (87),\ (72)$$

ersetzen; dabei ändert sich die Klasse dreimal, und die Wirkung ist die gleiche, als ob eine einmalige Änderung vorgenommen wäre. Das zum Beweise benutzte Prinzip gilt allgemein, und so ist der Satz bewiesen.

Aus ihm ergibt sich sofort: Eine Zahlfolge kann nur durch eine gerade Anzahl von Transpositionen in sich selbst übergehen. Denn eine ungerade Anzahl würde die Klasse ändern. — Weiter sehen wir:

Führt man durch Transpositionen eine Zahlfolge auf zwei Arten in eine andere über, so ist die Anzahl der Transpositionen entweder beide Male gerade oder beide Male ungerade; je nachdem beide Folgen zur gleichen Klasse gehören oder nicht.

§ 11. Hieraus folgt, daß bei allen Darstellungen einer Substitution durch eine Reihe von Transpositionen entweder stets eine gerade oder stets eine ungerade Anzahl von Transpositionen auftritt. Denn ist

$$s_i = \begin{pmatrix} 1, & 2, & 3, & \ldots, & n \\ i_1, & i_2, & i_3, & \ldots, & i_n \end{pmatrix},$$

so zeigt das letzte Theorem des vorigen Paragraphen, auf die beiden Zeilen von s_i angewendet, die Richtigkeit des Satzes.

Infolge seiner Gültigkeit kann man folgende Definition aufstellen: Eine Substitution gehört zur ersten oder zur zweiten Klasse, je nachdem sie sich aus einer geraden oder aus einer ungeraden Anzahl von Transpositionen zusammensetzt.

Die Einheitssubstitution gehört wegen

$$(a\,b) \cdot (a\,b) = 1$$

zur ersten Klasse.

Eine zyklische Substitution von m Elementen gehört zur ersten oder zur zweiten Klasse, je nachdem m ungerade oder gerade ist. Denn es ist ja

$$(a_1 a_2 a_3 \ldots a_m) = (a_1 a_2)(a_1 a_3) \ldots (a_1 a_m) .$$

Eine Substitution, die aus k Zykeln der Ordnungen bzw. $m_1, m_2, \ldots, m_k$ gebildet ist, gehört zur ersten oder zur zweiten Klasse, je nachdem die Summe

$$m_1 + m_2 + \ldots + m_k - k = \sum_{\alpha} (m_\alpha - 1)$$

$$(\alpha = 1, 2, \ldots, k)$$

gerade oder ungerade ist.

Das Produkt zweier Substitutionen gehört zur ersten oder zur zweiten Klasse, je nachdem beide Faktoren zur gleichen Klasse gehören oder nicht.

Ein Produkt von Substitutionen gehört zur ersten oder zur zweiten Klasse, je nachdem eine gerade oder eine ungerade Anzahl seiner Faktoren zur zweiten Klasse gehört.

In jeder Substitutionengruppe gehört entweder die Hälfte oder die Gesamtheit aller Substitutionen zur ersten Klasse. Denn sind $g_1, g_2, \ldots, g_\nu$ alle Substitutionen erster Klasse der Gruppe, und gibt es außer diesen ν Substitutionen erster Klasse auch nur noch eine andere zweiter Klasse, etwa u_1, so gehören alle Produkte $g_1 u_1, g_2 u_1, \ldots, g_\nu u_1$ zur zweiten Klasse; alle gehören nach I, § 1 zur Gruppe und sind nach II, § 1 voneinander verschieden. Also gehören mindestens so viel Substitutionen der Gruppe zur zweiten wie zur ersten Klasse. Dieselbe Schlußreihe kann man umgekehrt durchlaufen, indem man von allen Substitutionen $u_1, u_2, \ldots, u_\mu$ der zweiten Klasse ausgeht und mit einer beliebigen Substitution zweiter Klasse, etwa u', die Produkte $u'u_1, u'u_2, \ldots, u'u_\mu$ bildet. Man erkennt, daß mindestens so viele Substitutionen der Gruppe zur ersten wie zur zweiten Klasse gehören. Daraus folgt die behauptete Gleichheit beider Zahlen.

Auf die symmetrische Gruppe verwendet, liefert das den Satz: Es gibt ebensoviele Substitutionen erster wie zweiter Klasse von n Elementen, nämlich je $\frac{1}{2} n!$.

Die Substitutionen erster Klasse jeder Substitutionengruppe bilden eine Gruppe von halb so großer Ordnung oder die Gruppe selbst. Die Substitutionen erster Klasse von n Elementen bilden eine Gruppe der Ordnung $\frac{1}{2}n!$. Diese heißt die alternierende Substitutionengruppe der n Elemente. Bei $n = 3$ besteht sie für drei Elemente 1, 2, 3 aus den drei Substitutionen 1, (123), (132), wobei die alleinstehende 1 die identische Substitution bezeichnet; für $n = 4$ aus den zwölf Substitutionen erster Klasse

$$1\,,\ (123)\,,\ (124)\,,\ (132)\,,\ (134)\,,\ (142)\,,\ (143)\,,\ (234)\,,\ (243)\,,$$
$$(12)\,(34)\,,\ (13)\,(24)\,,\ (14)\,(23)\,.$$

Jede Substitutionengruppe von mehr als vier Elementen, die alle Substitutionen der Form $(a\,b)\,(c\,d)$ besitzt, enthält die alternierende Gruppe aller Elemente.

Zerlegen wir nämlich jede Substitution der alternierenden Gruppe in ein Produkt von Transpositionen, so tritt bei jeder Zerlegung eine gerade Anzahl von Transpositionen auf. Wir fassen sie von links beginnend in Paare von je zwei aufeinanderfolgenden zusammen. Diese Paare haben eine der Formen

$$(a\,b)\,(c\,d) \quad \text{oder} \quad (a\,b)\,(a\,c)\,.$$

Nach der Voraussetzung kommt das erste Paar unmittelbar in der Gruppe vor; das zweite mittelbar aber auch, weil die Umgestaltung gilt

$$(a\,b)\,(a\,c) = (a\,b)\,(d\,e) \cdot (d\,e)\,(a\,c)\,,$$

wo d, e von a, b, c verschiedene Elemente sind. Hierbei werden also fünf Elemente verwendet. Ist $n = 4$, so gibt es neben a, b, c kein solches Paar d, e; der Beweis wird hinfällig und der Satz selbst unrichtig, wie das Beispiel der Substitutionengruppe zeigt, die aus den vier Substitutionen besteht

$$1\,,\ (12)\,(34)\,,\ (13)\,(24)\,,\ (14)\,(23)\,.$$

Jede Substitutionengruppe, die alle Substitutionen der Form $(a\,b\,c)$ enthält, umfaßt die alternierende Gruppe aller ihrer Elemente. Denn es ist

$$(a\,b)\,(c\,d) = (a\,c\,b)\,(c\,b\,d) \quad \text{und} \quad (a\,b)\,(a\,c) = (a\,b\,c)\,.$$

§ 12. An die Möglichkeit, eine und dieselbe Substitution auf mehrfache Art durch Transpositionen darzustellen, knüpfen sich weitere interessante Untersuchungen an, von denen wir hier nur einige Ergebnisse anführen wollen. Sie beziehen sich auf die Anzahl der Darstellungen einer gegebenen Substitution durch das Produkt einer vorgeschriebenen Zahl von Transpositionen. Von Hurwitz stammt der folgende Satz:

Die Anzahl der Darstellungen einer aus n Elementen gebildeten Substitution als Produkt von v Transpositionen ist gleich

$$c_1 f_1^v + c_2 f_2^v + \dots + c_\varkappa f_\varkappa^v , \tag{7}$$

wo die $c_1, c_2, \dots, c_\varkappa$; $f_1, f_2, \dots, f_\varkappa$ von v nicht abhängen. Die Koeffizienten $c_1, c_2, \dots, c_\varkappa$ sind rationale, von der Substitution und der Zahl n abhängige Zahlen. Dagegen sind die $f_1, f_2, \dots, f_\varkappa$ ganze Zahlen, welche ausschließlich von n abhängen und folgendermaßen gebildet werden: Man zerlegt n auf alle möglichen Weisen in positive ganzzahlige Summanden

$$n = \nu_1 + \nu_2 + \dots + \nu_r \qquad (\nu_1 \geqq \nu_2 \geqq \nu_3 \geqq \dots \geqq \nu_r)$$

und setzt

$$f = \frac{\nu_1(\nu_1 - 1)}{2} + \frac{\nu_2(\nu_2 - 1)}{2} + \dots + \frac{\nu_r(\nu_r - 1)}{2}$$
$$- (\nu_1 + 2\nu_2 + 3\nu_3 + \dots) + n .$$

Die sämtlichen auf diese Weise gebildeten Zahlen f sind die oben mit $f_1, f_2, \dots, f_\varkappa$ bezeichneten. Dabei treten die von Null verschiedenen f ihrem absoluten Werte nach eine gerade Anzahl von Malen auf und zwar ebensooft positiv wie negativ.

§ 13. Wir kehren jetzt von den Untersuchungen über Substitutionen und Substitutionengruppen zu den allgemeinen in § 1 und § 2 definierten Gruppen zurück. Wir wollen sie zur Unterscheidung von den an eine bestimmte Darstellung der Operatoren geknüpften Gruppen als abstrakte Gruppen bezeichnen. Während bei den Substitutionengruppen ein einzelner Buchstabe ein Element und eine Substitution einen Operator bedeutete, soll hier bei den abstrakten Gruppen wieder unter einem Buch-

staben $a, b, c, \ldots$ ein Operator verstanden werden; die Klammern haben nun nicht mehr den Zweck, Zykeln anzugeben; es sind rein algebraische Zeichen.

Die Anzahl der Operatoren einer Gruppe $a, b, c, d, \ldots$ heißt ihre Ordnung (§ 3). Aus § 1, III entnehmen wir die Richtigkeit der Gleichungen

$$[(a\,b)\,c]\,d = (a\,b)\,(c\,d) = [a(b\,c)]\,d = a[b(c\,d)] = \ldots ;$$

man kann daher bei der Komposition von Operatoren, wie bei der gewöhnlichen Multiplikation, die sonst nötigen Klammern fortlassen; dagegen muß die Reihenfolge der Operatoren gewahrt bleiben.

Tritt in einer Gruppe ein Operator a auf, so kann man ihn mit sich selbst komponieren. Es kommt in der Gruppe also auch das Produkt von beliebig vielen ihm gleichen vor. Aus dem eben besprochenen Umstande folgt, daß man dabei

$$a \cdot a = a^2, \quad a \cdot a \cdot a = a^3, \quad a \cdot a \cdot a \cdot a = a^4, \quad \ldots, \quad a^\nu \cdot a = a^{\nu+1}$$

setzen kann, und daß für alle positiven μ, ν die Gleichung

$$a^\mu a^\nu = a^{\mu+\nu}$$

gilt. Wir wollen diese Produkte als Potenzen von a bezeichnen.

Die Ordnung der endlichen Gruppe G, zu der der Operator a gehört, sei n. Wir bilden mit ihm

$$a, \; a^2, \; a^3, \; a^4, \; \ldots, \; a^n, \; a^{n+1} ;$$

alle diese Potenzen gehören G an; also können sie wegen der Ordnung von G nicht sämtlich voneinander verschieden sein. Sei demnach die Beziehung vorhanden

$$a^\varkappa = a^{\varkappa+\lambda} \qquad (\varkappa, \; \varkappa + \lambda \leqq n + 1),$$

so folgt daraus jede der beiden Gleichungen

$$a^{\varkappa-1} \cdot a = a^{\varkappa-1}(a \cdot a^\lambda) \quad \text{und} \quad a \cdot a^{\varkappa-1} = (a^\lambda \cdot a) \cdot a^{\varkappa-1},$$

und nach § 1, II ergibt sich aus ihnen

$$(8) \qquad a \cdot a^\lambda = a, \quad a^\lambda \cdot a = a .$$

Nun werde mit b ein ganz beliebiger Operator von G bezeichnet und es werde gesetzt

$$x = b \cdot a^\lambda ; \quad y = a^\lambda \cdot b ,$$

dann liefert die Verwendung von (8) unter Berücksichtigung von II, § 1

$$x a = b \cdot a^\lambda a = b a \,; \quad \text{also} \quad x = b \,, \quad b \cdot a^\lambda = b \,;$$

$$a y = a^{\lambda+1} \cdot b = a b \,; \quad \text{also} \quad y = b \,, \quad a^\lambda \cdot b = b \,,$$

so daß also links- wie rechtsseitige Multiplikation eines beliebigen Operators b mit a^λ das b nicht ändert.

Wir bezeichnen $a^\lambda = e$ und nennen e den Einheitsoperator oder kürzer die Einheit. Jeder Operator b der endlichen Gruppe G liefert bei rechter wie bei linker Komposition mit e wieder b; d. h. es ist

(9) $$b e = b \quad \text{und} \quad e b = b \,.$$

Es gibt in G nur einen solchen Einheitsoperator. Denn wäre auch $b e_1 = b$, so hätte man

$$b e = b = b e_1 \,, \quad \text{also} \quad e = e_1 \,.$$

Diese Eigenschaften des Operators e zeigen die Berechtigung des ihm gegebenen Namens. Auch in dem besonderen Falle der Substitutionengruppen haben wir die Existenz eines solchen Einheitsoperators in Gestalt der identischen Substitution ermittelt, unabhängig von den jetzigen allgemeinen Betrachtungen.

Wir sahen, daß eine gewisse Potenz jedes Operators gleich der Einheit wird. Sei m der niedrigste Exponent von a, für den $a^m = 1$ wird. Dann folgt: Die Potenzen

(10) $$a \,,\ a^2,\ a^3,\ \ldots,\ a^{m-1},\ a^m = e = 1$$

sind untereinander verschieden. Denn aus einer Gleichung von der Form

$$a^\varkappa = a^{\varkappa+\lambda} \qquad (\varkappa \,,\ \lambda \leqq m)$$

würde $a^\lambda = 1 = e$ bei $\lambda < m$ folgen. Wir nennen m die Ordnung von a. Der einzige Operator von der Ordnung 1 ist die Einheit.

§ 14. Wie bei der Gruppe aller oder eines Teils aller Substitutionen, so können wir bei jeder abstrakten endlichen Gruppe zu jedem Operator a einen reziproken Operator oder eine Reziproke b ausfindig machen, d. h. einen, für den $a b = b a = 1$ wird. Offenbar ist

$b = a^{m-1}$, wenn m die Ordnung von a angibt, also $a^m = 1$ wird. Wir schreiben auch hier, wie in § 6,

(11) $$a^{m-1} = a^{-1}.$$

Da wir haben

$$(a\,b\,c \ldots e\,f) \cdot (f^{-1}\,e^{-1} \ldots c^{-1}\,b^{-1}\,a^{-1}) = 1 ,$$

so folgt für die Reziproke eines Produktes die Bestimmung

(12) $$(a\,b\,c \ldots e\,f)^{-1} = f^{-1}\,e^{-1} \ldots c^{-1}\,b^{-1}\,a^{-1}.$$

Ferner ist

(13) $$a^{-1} \cdot (a^{-1})^{-1} = e = a^{-1}\,a ,$$

also nach § 1, II: Die Reziproke zu a^{-1} ist a. Die Reziproke des Einheitsoperators e ist e selbst. Enthält eine endliche abstrakte Gruppe den Operator a, so auch seine Reziproke $a^{-1} = a^{m-1}$; eine jede enthält den zu sich selbst reziproken Einheitsoperator e.

Die Definition von $a^{-\varkappa}$ wird durch $(a^{-1})^{\varkappa}$ oder auch bei beliebigem λ durch

$$a^{-\varkappa} = a^{\lambda m - \varkappa}$$

geliefert, wo m die Ordnung von a ist.

Für die Potenzen eines Operators gilt das kommutative Gesetz.

§ 15. Gesetzt, die Ordnung m eines Operators d sei in zwei teilerfremde Faktoren zerlegbar, $m = m_1 \cdot \mu_1$. Wir bilden $d^{\mu_1} = d_1$ und $d^{m_1} = \delta_1$ von den Ordnungen m_1 und bzw. μ_1. Alle Potenzen von d_1 und alle von δ_1 kommen unter denen von d vor. Bilden wir, unter Beachtung, daß für die Potenzen von d das kommutative Gesetz gilt,

$$d_1^x\,\delta_1^y = d^{\mu_1 x + m_1 y} ,$$

so können wir, da μ_1, m_1 teilerfremd sind, x_0 und y_0 ganzzahlig so bestimmen, daß $\mu_1 x_0 + m_1 y_0 = 1$, also $d_1^{x_0}\,\delta_1^{y_0} = d$ wird. Man kann daher die Potenzen von d durch die Produkte der Potenzen von d_1 und von δ_1 ersetzen; und umgekehrt. Es ist dies gewissermaßen eine Zerlegung von d in Faktoren, die miteinander vertauschbar sind.

Ist weiter $\mu_1 = m_2 \cdot \mu_2$, wo m_2 und μ_2 teilerfremd

sind, so läßt sich δ_1 nach dem eben Besprochenen noch weiter zerlegen. Wir setzen

$$d_2 = \delta_1^{\mu_2} = d^{m_1 \mu_2} = d^{m:m_2}; \quad \delta_2 = \delta_1^{m_2} = d^{m_1 m_2} = d^{m:\mu_2},$$

so daß d_2 und δ_2 die Ordnungen m_2 bzw. μ_2 haben; dann können wir δ_1 in d_2 und δ_2 zerlegen, also d in d_1, d_2, δ_2 mit den Ordnungen m_1, m_2, $\frac{m}{m_1 \cdot m_2}$. So gehen wir weiter und gelangen zu dem Satz: Ist die Ordnung m eines Operators d, in ihre verschiedenen Primzahlpotenzen zerlegt, gleich $p^\alpha q^\beta r^\gamma \ldots$, und setzen wir

$$m = p^\alpha \cdot \pi = q^\beta \cdot \varkappa = r^\gamma \cdot \varrho = \ldots$$

sowie

$$d^\pi = d_1, \quad d^\varkappa = d_2, \quad d^\varrho = d_3, \quad \ldots,$$

so kann man die Potenzen von d durch die von d_1, d_2, d_3, ... ersetzen. Dabei haben d_1, d_2, d_3, ... als Ordnungen die Primzahlpotenzen p^α, q^β, r^γ, ... Für die Operatoren d_1, d_2, d_3, ... gilt das kommutative Gesetz; denn sie sind Potenzen von d, und für d^α, d^β gilt $d^\alpha d^\beta = d^\beta d^\alpha$.

Eine solche Zerlegung der Operatoren d in d_1 und δ_1 ist bei vorgeschriebenen, teilerfremden Ordnungen m_1 und μ_1 und bei Gültigkeit des kommutativen Gesetzes für die Faktoren nur auf die angegebene eine Art möglich. Denn aus der Annahme $d_1^{x_0} = d_0$, $\delta_1^{y_0} = \delta_0$ und

$$d = g_1 \cdot \gamma_1 \quad \text{bei} \quad g_1^{m_1} = 1, \; \gamma_1^{\mu_1} = 1 \quad \text{und} \quad g_1 \gamma_1 = \gamma_1 g_1$$

folgt der Reihe nach, wenn die Zahlen x_0, y_0 die obige Bedeutung haben, so daß $\mu_1 x_0 + m_1 y_0 = 1$ ist,

$$g_1 \gamma_1 = d_0 \delta_0 = d; \quad g_1^{\mu_1} \gamma_1^{\mu_1} = d_0^{\mu_1} \delta_0^{\mu_1}; \quad g_1^{\mu_1} = d_0^{\mu_1};$$

$$g_1^{\mu_1 x_0} = d_0^{\mu_1 x_0}; \quad g_1^{1 - m_1 y_0} = d_0^{1 - m_1 y_0}; \quad g_1 = d_0.$$

Ebenso ergibt sich $\gamma_1 = \delta_1$. Die Zerlegung ist also eindeutig; und was für zwei Faktoren bewiesen ist, gilt ebenso von mehreren. Daß in dem eben geführten Beweise

$$(g_1 \gamma_1)^{\mu_1} = g_1^{\mu_1} \gamma_1^{\mu_1}$$

gesetzt werden durfte, folgt aus der Tatsache, daß für g_1 und γ_1 das kommutative Gesetz gilt. Denn das liefert

$$(g_1 \gamma_1)^2 = g_1(\gamma_1 g_1) \gamma_1 = g_1(g_1 \gamma_1) \gamma_1 = g_1^2 \gamma_1^2 ,$$

$$(g_1 \gamma_1)^3 = (g_1^2 \gamma_1^2) (g_1 \gamma_1) = g_1^2 \gamma_1^1(\gamma_1 g_1) \gamma_1 = g_1^2 \gamma_1 g_1 \gamma_1^2 = g_1^3 \gamma_1^3 ,$$

usw.

---

2. Kapitel.

Das Cayleysche Quadrat.

§ 16. Wir bezeichnen die aus den Operatoren

$$1, a, b, c, \ldots, d, f$$

gebildete Gruppe G durch das Symbol einer eckigen Klammer, die alle Operatoren enthält; wir schreiben also:

$$G = [1, a, b, c, \ldots, d, f] .$$

Die 1 soll den Einheitsoperator darstellen.

Über die Konstitution einer Gruppe G erhält man am einfachsten und vollständigsten in folgender Weise eine Einsicht: Wir ordnen die Produkte aus je zwei Operatoren in ein quadratisches Schema ein:

	1	a	b	c	...	d	f
1	$1 \cdot 1$	$1 \cdot a$	$1 \cdot b$	$1 \cdot c$	...	$1 \cdot d$	$1 \cdot f$
a	$a \cdot 1$	$a \cdot a$	$a \cdot b$	$a \cdot c$	...	$a \cdot d$	$a \cdot f$
b	$b \cdot 1$	$b \cdot a$	$b \cdot b$	$b \cdot c$	...	$b \cdot d$	$b \cdot f$
c	$c \cdot 1$	$c \cdot a$	$c \cdot b$	$c \cdot c$	...	$c \cdot d$	$c \cdot f$
..	. .	. .	. .	. .	. . .	. .	. .
d	$d \cdot 1$	$d \cdot a$	$d \cdot b$	$d \cdot c$	...	$d \cdot d$	$d \cdot f$
f	$f \cdot 1$	$f \cdot a$	$f \cdot b$	$f \cdot c$	...	$f \cdot d$	$f \cdot f$

und ersetzen die unausgeführten Produkte im Innern des Schemas durch ihre nach § 1, I bestimmten Werte, die durch die Konstitutionsvorschriften der Gruppe gegeben sein müssen. Der Eingang links durch die erste Spalte gibt den linken, der Eingang oben durch die erste Zeile

den rechten Faktor der Komposition; der Treffpunkt von Zeile und Spalte das Produkt.

Als einfaches Beispiel wählen wir die Gruppe sechster Ordnung mit den Operatoren

$$a = 1, \quad b, \quad c = b^2, \quad d = b^3, \quad f = b^4, \quad g = b^5; \quad (b^6 = 1).$$

In dieser Darstellung der Operatoren als Potenzen von b liegen alle Kompositionsvorschriften, und wir können ohne weiteres das quadratische Schema für diese Gruppe bilden

(1)

	a	b	c	d	f	g
a	a	b	c	d	f	g
b	b	c	d	f	g	a
c	c	d	f	g	a	b
d	d	f	g	a	b	c
f	f	g	a	b	c	d
g	g	a	b	c	d	f.

Ein zweites Beispiel liefere die Gruppe mit den acht Operatoren $1, a, b, c, d, e, f, g$ und dem Schema, aus dem umgekehrt die Kompositionsvorschriften zu entnehmen sind,

(2)

	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	1	c	b	g	f	e	d
b	b	c	1	a	f	g	d	e
c	c	b	a	1	e	d	g	f
d	d	f	g	e	1	c	a	b
e	e	g	f	d	c	1	b	a
f	f	d	e	g	b	a	c	1
g	g	e	d	f	a	b	1	c.

Hieraus ersieht man z. B., daß a, b, c, d, e von der Ordnung 2 sind, während f, g die Ordnung 4 haben.

Auf solche Tabellen hat Cayley zuerst hingewiesen; sie heißen nach ihm Cayleysche Tabellen oder

Cayleysche Quadrate. Die Anordnung der Operatoren in der horizontalen und in der vertikalen Eingangsreihe ist beliebig; die Anordnung in den Innenreihen ist nach § 1, II und III bestimmten Beschränkungen unterworfen. So liefert II unmittelbar den Satz: in keiner Zeile und in keiner Spalte einer Cayleyschen Tabelle darf ein Operator mehrfach vorkommen, oder positiv ausgedrückt: jede Zeile und jede Spalte enthält alle Operatoren der Gruppe.

Schon hieraus erhält man eine obere Grenze für die Anzahl aller möglichen Gruppen von n Operatoren. Bei der Ausfüllung der Tabelle ist nämlich die hinter 1 stehende erste Zeile und die unter 1 stehende erste Spalte durch die Eingangszeile und -spalte fest bestimmt. Ferner ist die letzte Zeile wegen II, § 1 durch die $(n-1)$ vorhergehenden bestimmt; und Entsprechendes gilt für die letzte Spalte, indem Zeile wie Spalte den in den voraufgehenden Reihen noch fehlenden Operator enthalten müssen. Für jede einzelne Zeile gibt es, wenn man die übrigen Zeilen mit ihren Einwirkungen außer acht läßt, $(n-1)!$ Ausfüllungsmöglichkeiten, also im ganzen als obere Grenze für die Anzahl der Gruppen $n$ter Ordnung

$$[(n-1)!]^{n-2}.$$

Diese läßt sich leicht noch weiter herabdrücken, doch gehen wir darauf nicht ein. Man kann die Anordnung in den Eingangsreihen so treffen, daß die Diagonale des Quadrats, die von links oben nach rechts unten läuft, nur Einheitsoperatoren enthält.

Die nur durch I und II, § 1 bestimmten quadratischen Schemata heißen nach Euler lateinische Quadrate. Für $n=3$ gibt es nur ein solches, nämlich

$$\begin{matrix} a & b & c \\ b & c & a \\ c & a & b \end{matrix},$$

wenn die erste Zeile und Spalte als gegeben angesehen werden. Für $n=4$ gibt es unter der gleichen Voraussetzung vier lateinische Quadrate

a	*b*	*c*	*d*		*a*	*b*	*c*	*d*		*a*	*b*	*c*	*d*		*a*	*b*	*c*	*d*
b	*a*	*d*	*c*		*b*	*a*	*d*	*c*		*b*	*c*	*d*	*a*		*b*	*d*	*a*	*c*
c	*d*	*a*	*b*		*c*	*d*	*b*	*a*		*c*	*d*	*a*	*b*		*c*	*a*	*d*	*b*
d	*c*	*b*	*a*,		*d*	*c*	*a*	*b*,		*d*	*a*	*b*	*c*,		*d*	*c*	*b*	*a*.

Beim Übergange vom lateinischen Quadrate zum Cayleyschen ist § 1, III zu beachten. Die dadurch gelieferte Beschränkung läßt keine so anschauliche Deutung zu, wie II, § 1. Sie ist aber zu berücksichtigen, da es lateinische Quadrate gibt, bei denen III nicht erfüllt ist. So tritt schon bei dem Schema eines lateinischen Quadrates von fünf Elementen, als Gruppenquadrat aufgefaßt,

	1	*a*	*b*	*c*	*d*
1	1	*a*	*b*	*c*	*d*
a	*a*	*c*	1	*d*	*b*
b	*b*	*d*	*a*	1	*c*
c	*c*	*b*	*d*	*a*	1
d	*d*	1	*c*	*b*	*a*,

das die Forderungen I und II erfüllt, gleichwohl der Widerspruch auf

$$(a\,b)\,c = 1 \cdot c = c\,, \quad a(b\,c) = a \cdot 1 = a\,,$$

o daß III nicht erfüllt wird, das Schema also keine abstrakte Gruppe gibt, deren Operatoren a und c verschieden wären.

§ 17. Wir wollen nun die Gruppen der niedrigsten Ordnungen bestimmen.

I. Für $n = 2$ gibt es nur ein Schema für eine abstrakte Gruppe, nämlich

	1	*a*
1	1	*a*
a	*a*	1;

die Operatoren sind 1, a und es ist $a^2 = 1$.

II. Für $n = 3$ bilden wir zunächst das unvollständige Schema

	1	*a*	*b*
1	1	*a*	*b*
a	*a*	*	*
b	*b*	*	*

und versuchen die mit Sternchen versehenen, noch offenen Stellen passend auszufüllen. Dabei könnte $a \cdot a = 1$ oder $= b$ sein. Träte das erste auf, so würde für $a\,b$ nur b übrig bleiben, das würde aber nach II, § 1 auf $a = 1$ führen. Wir müssen daher $a \cdot a = b$, $a \cdot b = 1$ setzen und erhalten dann das vollständige Schema der Gruppe

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a,

das die Operatoren $1, a, b = a^2$ mit $a^3 = 1$ liefert; III, § 1 ist hier erfüllt.

III. Für die weiteren Konstruktionen wollen wir einen fundamentalen, erst später zu beweisenden Satz bereits hier verwenden: Enthält die Gruppe G den Operator a, dann ist die Ordnung von G ein Vielfaches der Ordnung von a. Infolgedessen kann G nur Operatoren enthalten, deren Ordnungen Teiler der Ordnung von G sind. Demnach können bei der Ordnung 4 von G die Ordnungszahlen der Operatoren nur 1, 2 oder 4 sein. Es kann als Operator der Ordnung 1 lediglich der Einheitsoperator vorkommen (§ 13, S. 17). Kommt ein Operator der Ordnung 4 vor, so enthält G die Potenzen von a, nämlich a, a^2, a^3, $a^4 = 1$, und es gibt weiter keine Operatoren in G. Die Konstruktion des Cayleyschen Quadrates ist daher einfach.

Hier wäre also ein Typus einer Gruppe der Ordnung 4 gewonnen. Wir untersuchen, ob es noch andere gibt.

Haben alle Operatoren von G außer $e = 1$ die Ordnung 2, so ist

$$a\,a = 1, \quad b\,b = 1, \quad c\,c = 1$$

und auch

$$(a\,b)\,(a\,b) = 1, \quad (b\,a)\,(b\,a) = 1 .$$

$a\,b$ kann nicht $= a$ sein (§ 1, II), ebensowenig $= b$ oder $= 1$ wegen $a\,b = 1 = a\,a$. Da $a\,b$ einem der Operatoren a, b, c, $e = 1$ gleich sein muß (§ 1, I), so bleibt nur $a\,b = c$ übrig und ebenso $b\,a = c$, $a\,c = b$, $b\,c = a$, $c\,b = a$. Hier-

nach erhalten wir die sogenannte Vierergruppe mit dem Cayleyschen Quadrate

(3)

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1.

Für $n = 4$ bestehen also zwei wesentlich verschiedene Gruppentypen und nur zwei.

IV. Unser Hilfssatz zeigt, daß für $n = 5$ außer der Einheit noch ein Operator fünfter Ordnung vorhanden ist. Dieser heiße a; dann wird die Gruppe

$$G = [1, a, a^2, a^3, a^4].$$

V. Für $n = 6$ gibt es in der Gruppe nur Operatoren von einer der Ordnungen 1, 2, 3, 6. Kommt ein Operator a der Ordnung 6 vor, so wird genau wie bei IV die Gruppe

(4) $$G_1 = [1, a, a^2, a^3, a^4, a^5].$$

Wir untersuchen, ob außer diesem G_1 noch andere Gruppen mit der Ordnung $n = 6$ gebildet werden können. Zunächst fragen wir, ob alle Operatoren der Gruppe außer der Einheit $e = 1$ von zweiter Ordnung sein können. Die sechs Operatoren seien $e = 1$, a, b, c, d, f, und es gelte der Annahme gemäß die Reihe der Gleichungen

$$a^2 = 1, \quad b^2 = 1, \quad c^2 = 1, \quad \ldots, \quad (ab)^2 = 1, \quad (ba)^2 = 1,$$
$$(ac)^2 = 1, \quad (ca)^2 = 1, \quad \ldots,$$

also auch, wie aus ihnen folgt,

$$a^{-1} = a, \quad b^{-1} = b, \quad c^{-1} = c, \quad \ldots, \quad (ab)^{-1} = ab,$$
$$(ba)^{-1} = ba, \quad (ac)^{-1} = ac, \quad \ldots$$

Nun kann wegen II, § 1 das Produkt ab weder $=a$ noch $=b$ noch $=1=a^2$ sein; ab wird also $=c$ oder $=d$ oder $=f$ sein. Wir wählen die Bezeichnung so, daß $ab = c$ ist; hierin ist keine Beschränkung enthalten. Dann wird man schließen können

$$ac = a \cdot ab = b, \quad cb = ab \cdot b = a,$$
$$ba = b^{-1}a^{-1} = (ab)^{-1} = ab = c.$$

Hiernach beginnen wir die Aufstellung der Cayleyschen Tabelle in der Form

	1	a	b	ab	d	f
1	1	a	b	ab	d	f
a	a	1	ab	b	*	*
b	b	ab	1	a	*	* .

Hier müßten die Sternchen in der zweiten wie die in der dritten Zeile durch die in diesen beiden Zeilen noch nicht vorkommenden Operatoren d und f ausgefüllt werden; das läßt sich hinsichtlich der Spalten ohne Verletzung von § 1, II nicht bewerkstelligen. Eine Gruppe der Ordnung 6 mit lauter Operatoren zweiter Ordnung neben der Einheit ist also unmöglich.

Gibt es daher außer G_1 noch weitere Gruppen der Ordnung 6, so enthalten sie sicher mindestens einen Operator der Ordnung 3. Der heiße a; dann können wir die sechs Operatoren durch $1, a, a^2, b, c, d$ darstellen. Das Produkt ab kann wegen II, § 1 nicht $=1, a, b, a^2$ sein, ist also $=c$ oder d. Wir bezeichnen $ab=c$; dann kann a^2b nicht $1, a, b, a^2, ab=c$ sein; also wird $a^2b=d$. Die Gruppe besteht dann aus den sechs Operatoren

$$1,\ a,\ a^2,\ b,\ ab,\ a^2b \qquad (a^3=1).$$

Unter diesen muß b^2 vorkommen; b^2 kann aber nicht $=b, ab, a^2b$ sein; b^2 wird also zu einem der Operatoren $1, a, a^2$. Aus $b^2=a$ würde folgen

$$b=b,\quad b^2=a,\quad b^3=ab,\quad b^4=a^2,\quad b^5=a^2b,\quad b^6=1,$$

d. h. der Operator b wäre von der sechsten Ordnung, und wir kämen auf die Gruppe G_1. Gleiches würde aus $b^2=a^2$ folgen. Es muß also $b^2=1$ gesetzt werden.

Unter unseren Operatoren kommt nach I, § 1 auch ba vor; das kann nicht $=1, a, a^2$ oder b sein, und es bleibt uns nur ab oder ab^2 zur Wahl. Aus der ersten Annahme folgt

$$ba=ab,\ (ba)^2=ba\cdot ba=ab\cdot ba=a^2,\ (ba)^3=ba\cdot a^2=b,$$
$$(ba)^4=a^2\cdot a^2=a,\ (ba)^5=a\cdot ba=a^2b,\ (ba)^6=b^2=1;$$

die Gruppe bestände also wieder aus den Potenzen eines

einzigen Operators und wäre mit G_1 identisch. Es ist demnach nur die Annahme $b\,a = a^2 b$ bei $a^3 = 1$ und $b^2 = 1$ zu untersuchen. Hierfür ergibt sich ohne jede Schwierigkeit das quadratische Schema Cayleys widerspruchsfrei, unter Erfüllung von III, § 1 einer Gruppe G_2

(5)

	1	a	a^2	b	ab	a^2b
1	1	a	a^2	b	ab	a^2b
a	a	a^2	1	ab	a^2b	b
a^2	a^2	1	a	a^2b	b	ab
b	b	a^2b	ab	1	a^2	a
ab	ab	b	a^2b	a	1	a^2
a^2b	a^2b	ab	b	a^2	a	1.

Für $n = 6$ gibt es also zwei wesentlich voneinander verschiedene Gruppentypen und nur zwei.

Wohl zu merken ist freilich, daß hier wie in den früheren Beispielen die Resultate zu ihrer Sicherstellung noch des Nachweises der Gültigkeit des assoziativen Gesetzes bedürfen.

VI. Die Behandlung der Gruppen von der Ordnung 7 stößt, wie bei der Ordnung 3 und 5 und allgemein bei jeder Primzahlordnung, auf keine Schwierigkeiten.

§ 18. Mit dem Cayleyschen Schema steht eine merkwürdige Substitutionengruppe in engem Zusammenhange. Wir gehen zunächst auf ihre Bildung und auf ihre Haupteigenschaften ein.

Wir greifen aus dem Cayleyschen Quadrate zwei Zeilen in ihrer nicht reduzierten Form heraus, etwa die mit den Anfangsoperatoren g und h,

	1	a	b	c	d	$\dots$
g	g	$g \cdot a$	$g \cdot b$	$g \cdot c$	$g \cdot d$	$\dots$
h	h	$h \cdot a$	$h \cdot b$	$h \cdot c$	$h \cdot d$	$\dots$

$(g,\, h = 1, 2, 3, \dots)$

und ordnen diesen Zeilen mit den Eingängen g, h bzw. die Substitutionen

$$s_g = \begin{pmatrix} g & g\,a & g\,b & g\,c & g\,d & \dots \\ 1 & a & b & c & d & \dots \end{pmatrix} = |g\,\varrho,\, \varrho|,$$

$$s_h = \begin{pmatrix} h & h\,a & h\,b & h\,c & h\,d & \dots \\ 1 & a & b & c & d & \dots \end{pmatrix} = |h\,\varrho,\, \varrho|$$

zu. Dann ergibt sich als Produkt der Substitutionen

$$s_g \cdot s_h = |g\varrho, \varrho| \cdot |h\varrho, \varrho| = |gh\varrho, h\varrho| \cdot |h\varrho, \varrho| \\ = |gh\varrho, \varrho|;$$

diese Substitution ist nach der angegebenen Bildung gleich s_{gh}, d. h. die des Cayleyschen Quadrats, die der Zeile mit gh als dem linken Eingangsoperator entspricht. Es ist daher

$$s_g \cdot s_h = s_{gh}.$$

Also ist für die s_a die Bedingung I aus § 1 erfüllt, und der Komposition der Operatoren g und h entspricht die der Substitutionen s_g und s_h. Demnach gilt auch II und III, § 1, und die s_a bilden eine Substitutionengruppe, die von gleicher Konstitution ist, wie die Gruppe der Operatoren $1, a, b, c, d, \ldots$ Der Ausdruck „gleiche Konstitution“ soll bald genauer erklärt werden.

Die erhaltene Substitutionengruppe hat gleiche Ordnungs- und Gradzahl; denn jeder der n Zeilen der n Operatoren entspricht eine Substitution von n Elementen. Jede Substitution der Gruppe außer der Einheit setzt alle ihre Elemente um; denn in keiner Spalte steht das gleiche Element zweimal. Jede Substitution besteht aus Zyklen von gleicher Ordnung; denn sonst würde es eine von 1 verschiedene Potenz der Substitution geben, die weniger als n Elemente umsetzt; käme z. B. die Substitution $s = (ab)(cde)$ vor, so müßte auch $s^2 = (ced)$ vorhanden sein, was dem eben Bewiesenen widerspräche. Gruppen mit der Eigenschaft, gleiche Ordnungs- und Gradzahl zu haben, heißen reguläre Substitutionengruppen.

So kann man also von einer abstrakten Gruppe zu einer Substitutionengruppe kommen. Umgekehrt kann natürlich jede Substitutionengruppe als abstrakte Gruppe dargestellt werden, indem man die Substitutionen selbst als Operatoren der Gruppe auffaßt. Man kann dabei die Cayleysche Tabelle ohne weiteres bilden. —

Wir betrachten als Beispiel die zweite der in § 16 (S. 21) aufgestellten Tabellen. Sie liefert die Substitutionengruppe (in der 1 und nicht e der Einheitsoperator ist)

$s_1 = 1$, $s_a = (1a)(bc)(ef)(dg)$, $s_b = (1b)(ac)(df)(eg)$,

$$s_c = (1c)(ab)(de)(fg)\,,\quad s_d = (1d)(af)(bg)(ce)\,,$$
$$s_e = (1e)(ag)(bf)(cd)\,,\quad s_f = (1gcf)(aebd)\,,$$
$$s_g = (1fcg)(adbe)\,;$$

an ihr finden sich alle vorher abgeleiteten Eigenschaften bestätigt.

Geht man andererseits von der folgenden Gruppe von Substitutionen

$$t_1 = 1\,,\quad t_a = (12)\,,\quad t_b = (34)\,,\quad t_c = (12)(34)\,,$$
$$t_d = (13)(24)\,,\quad t_e = (14)\,23)\,,\quad t_f = (1324)\,,\quad t_g = (1423)$$

zum Cayleyschen Quadrate über und schreibt statt t_1, t_a, t_b, ... t_f, t_g kürzer nur $1, a, b, \ldots f, g$, faßt also die Indizes der t als Operatoren auf, so kommt man genau wieder auf das Quadrat (2), § 16 zurück. Das zeigt, daß dieselbe abstrakte Gruppe zu mehreren, ihren Graden nach verschiedenen Substitutionengruppen von gleicher Konstitution führen kann.

§ 19. Es ist nicht nötig für die Erkenntnis der Natur einer abstrakten Gruppe, alle Zeilen ihres Cayleyschen Quadrates anzugeben, da meistens einige aus anderen abgeleitet werden können. Ist z. B.

	1	a	b	c	d	f	g	...
a	a	a^2	ab	ac	ad	af	ag	...

gegeben, so ist auch die Zeile

a^2	a^2	a^3	$a(ab)$	$a(ac)$	$a(ad)$	$a(af)$	$a(ag)$	...

unmittelbar bekannt.

Diese Bemerkung führt zu der Aufgabe, eine Gruppe durch möglichst wenige Angaben vollständig zu bestimmen.

Gewisse Gruppen lassen sich aus einem einzigen Operator ableiten, dessen Ordnung gegeben ist. So wird (1) § 16 durch den Operator b, für den $b^6 = 1$ ist, während seine niedrigeren Potenzen von 1 verschieden sind, durchaus bestimmt. Wir schreiben das gelegentlich

$$b^6 = 1 \quad (6\,\text{min})\,,$$

wo die Klammer andeuten soll, daß der Exponent 6 der

kleinste ist, für den die Gleichung gilt. Solchen Gruppen sind wir auch in § 17 begegnet. Ist a^m die niedrigste Potenz des Operators a, die $=1$ wird, so kann die Cayleysche Tabelle in die gedrängte Form

	a^k
a^h	a^{h+k}

$(a^m = 1)$

gebracht werden, falls jeder Exponent $h+k$, der größer als $m-1$ ist, durch seinen kleinsten nicht negativen Rest modulo m ersetzt wird. Solche Gruppen heißen zyklische Gruppen; sie bestehen aus den verschiedenen Potenzen eines Operators und haben die gleiche Ordnung wie dieser. Man kann eine solche Gruppe freilich auch in anderer Art charakterisieren, wenigstens wenn die Ordnung der Gruppe mehr als einen Primfaktor enthält, wie das aus § 14 hervorgeht.

Hierdurch werden wir darauf geführt, endliche Gruppen aus zwei verschiedenen Operatoren a, b von gegebenen Ordnungen h, k zu bilden. Dabei reicht aber eine Festsetzung von der Form

(6) $$a^h = 1\,,\quad b^k = 1 \qquad (h\,,\ k \min)$$

nicht aus. Besteht nämlich kein weiterer Zusammenhang zwischen den Operatoren a und b, so sind unter anderen die Kompositionsresultate

$$ab\,,\ aba\,,\ abab\,,\ ababa\,,\ \ldots$$

Operatoren der Gruppe, die sich nicht reduzieren lassen. Man hat somit beliebig viele voneinander verschiedene Operatoren der Gruppe, und diese ist demnach von unendlich hoher Ordnung.

Es ist also für endliche Gruppen außer den Beziehungen (6) noch eine weitere nötig. Lautet diese einfach auf die Erfüllung des kommutativen Gesetzes, nämlich

(7) $$ba = ab\,,$$

so erhält man stets eine endliche Gruppe. Denn die wiederholte Verwendung von (7) liefert eine Reihe von Gleichungen

$$ba^2 = ba \cdot a = ab \cdot a = a \cdot ba = a^2 b\,;$$

$$b^2 a = bb \cdot a = b \cdot ab = ba \cdot b = ab^2\,;\ \ldots$$

$$b^\mu a^\lambda = a^\lambda b^\mu\,;\quad a^\lambda b^\mu a^{\lambda_1} b^{\mu_1} \ldots = a^{\lambda+\lambda_1+\cdots} b^{\mu+\mu_1+\cdots}\,;$$

d. h. ein jedes Kompositionsresultat oder jeder Operator der Gruppe kann auf die Form $a^\sigma b^\tau$ gebracht werden und wegen (6) auf die einfachere

(8) $a^\varrho b^\sigma \quad (\varrho = 0, 1, 2, \ldots h-1; \; \sigma = 0, 1, 2, \ldots k-1)$.

Die Ordnung der Gruppe ist sonach höchstens $h \cdot k$.

Statt (7) können zu (6) andere Relationen treten. So ist die Gruppe (2), § 16, durch die drei Beziehungen

(9) $$a^2 = 1, \quad f^4 = 1, \quad fa = af^3 \qquad (2, 4 \min)$$

charakterisiert; a^2 ist dabei die niedrigste Potenz von a und f^4 die niedrigste Potenz von f, die $=1$ werden. Man erkennt leicht, daß auch die allgemeinere Annahme

(10) $$a^h = 1; \quad b^k = 1; \quad ba = ab^l \qquad (h, k \min)$$

stets auf eine endliche Gruppe führt, da jedes $b^\alpha a^\beta$ auf die Form $a^\gamma b^\delta$ gebracht werden kann, indem man die letzte der Gleichungen (10) mehrfach anwendet.

Wollte man allgemein versuchen, in die Behandlung von Gruppen einzutreten, die durch

(11) $$a^\alpha = 1, \quad b^\beta = 1, \quad ba = a^\mu b^\nu$$

definiert sind, so wäre die erste Frage die, welche Werte μ und ν haben dürfen, um eine endliche Gruppe widerspruchfrei zu liefern. Eine durch (11) gelieferte Gruppe könnte dann weiter auch dadurch banal werden, daß aus den Annahmen sich Beziehungen ergäben, die nur durch $a = b$ zu befriedigen sind; denn daß sich dabei jede mögliche Annahme (11) verwirklicht, ist klar. Alle diese Untersuchungen führen auf beträchtliche Schwierigkeiten. Wir wollen uns damit begnügen, einige hierher gehörige Beispiele zu behandeln.

§ 20. Es sei zunächst

$$a^3 = 1; \quad b^4 = 1; \quad ba = a^2 b^2 .$$

Dabei seien a^3 und b^4 die niedrigsten Potenzen von a und b, die $=1$ werden. Dann folgt

$$aba = a \cdot a^2 b^2 = a^3 b^2 = b^2 ,$$

und weiter ergeben sich die beiden Gleichungen für den Operator $b^3 a^2 b^3$

$$b^3 a^2 b^3 = b \cdot b^2 \cdot a^2 b^3 = b \cdot a\, b\, a \cdot a^2 b^3 = b\, a\, b \cdot a^3 \cdot b^3$$
$$= b\, a\, b^4 = b\, a\,,$$
$$b^3 a^2 b^3 = b^3 a^2 \cdot b^2 \cdot b = b^3 a^2 \cdot a\, b\, a \cdot b = b^3 \cdot a^3 \cdot b \cdot a\, b$$
$$= b^4 a\, b = a\, b\,.$$

Also ist hieraus zunächst zu schließen $a\,b = b\,a$ und daraus weiter

$$a^2 b^2 = b\, a = a\, b\,; \quad a^{-1} \cdot a^2 b^2 \cdot b^{-1} = a^{-1} \cdot a\, b \cdot b^{-1}\,; \quad a\, b = 1\,;$$
$$b = a^{-1} = a^2\,; \quad b^8 = a^{16} = a = 1\,,$$

und das verstößt gegen die Annahme, daß a von der Ordnung 3 ist.

§ 21. Ein Beispiel für die Erzeugung unendlicher Gruppen liefert die Annahme

(12) $$a^4 = 1\,; \quad b^4 = 1\,; \quad b\, a = a^3 b^3\,,$$

wo a und b von der vierten Ordnung sein sollen. Wir können die Operatoren dieser Gruppe in folgender Weise repräsentieren, wobei u eine unbestimmte Größe bedeutet:

(13) $$a = |u,\, iu|\,, \quad b = |u,\, iu + 1 - i|\,; \quad \left(i = \sqrt{-1}\right);$$

denn durch (13) sind alle Bedingungen (12) erfüllt, da man hat

$$a^2 = |u,\, iu| \cdot |u,\, iu| = |u,\, iu| \cdot |iu,\, -u| = |u,\, -u|\,,$$
$$a^3 = |u,\, -u| \cdot |u,\, iu| = |u,\, -u| \cdot |-u,\, -iu| = |u,\, -iu|\,,$$
$$a^4 = |u,\, -iu| \cdot |u,\, iu| = |u,\, -iu| \cdot |-iu,\, u| = |u,\, u| = 1\,;$$
$$b^2 = |u,\, iu + 1 - i| \cdot |u,\, iu + 1 - i|$$
$$= |u,\, iu + 1 - i| \cdot |iu + 1 - i,\, -u + 2| = |u,\, -u + 2|\,,$$
$$b^3 = |u,\, -u + 2| \cdot |u,\, iu + 1 - i|$$
$$= |u,\, -u + 2| \cdot |-u + 2,\, -iu + 1 + i|$$
$$= |u,\, -iu + 1 + i|\,,$$
$$b^4 = |u,\, -u + 2| \cdot |u,\, -u + 2|$$
$$= |u,\, -u + 2| \cdot |-u + 2,\, u| = |u,\, u| = 1\,;$$
$$b\, a = |u,\, iu + 1 - i| \cdot |u,\, iu| = |u,\, -u + 1 - i|\,,$$
$$a^3 b^3 = |u,\, -iu| \cdot |u,\, -iu + 1 + i| = |u,\, -u + 1 - i|\,.$$

Es ist daher (13) eine Repräsentation von (12), derart,

daß die Operatoren beider Gruppen sich gegenseitig entsprechen. Dabei können verschiedenen Operatoren von (12) allenfalls gleiche von (13) entsprechen, aber gleichen von (12) nicht verschiedene von (13). Ist also (13) von unendlich hoher Ordnung, so auch (12).

Nun wird, wie sich sofort ergibt,

$$a^2 b^2 = |u, -u| \cdot |u, -u+2| = |u, -u| \cdot |-u, u+2|,$$

$$(a^2 b^2)^m = |u, u+2m|,$$

und $a^2 b^2$ ist von unendlich hoher Ordnung, da $u+2m$ für kein m den Wert u wieder annimmt. Deshalb sind auch (13) und (12) von unendlich hoher Ordnung.

Man kann die Darstellung (13) leicht geometrisch deuten. Wir nehmen in der Ebene der x, y einen Punkt O als Anfangspunkt eines rechtwinkligen Koordinatensystems an und auf der x-Achse in der Entfernung 1 den Einheitspunkt Q. Einem beliebigen Punkte P geben wir die Koordinaten x und y und schreiben $P=(x, y)$.

Nun deuten wir den Operator a als die Operation, die P auf dem, um O mit OP geschlagenen Kreise in positivem Sinne um einen Quadranten weiterführt. Dadurch ist $a^4=1$ erfüllt. — Den Operator b deuten wir als die Operation, die P auf dem, um Q mit QP geschlagenen Kreise in positivem Sinne um einen Quadranten weiterführt. Dadurch ist $b^4=1$ erfüllt. Geometrisch erkennt man leicht, daß auch die dritte Forderung (13) erfüllt ist. — Diese geometrische Deutung fällt mit (13) zusammen, wenn man für u den Ausdruck $x+iy$ setzt.

Bei unserer Repräsentation wandelt sich durch die Operation a^2 der Punkt $P=(x, y)$ in $P_1=(-x, -y)$ um und durch b^2 wird P_1 in $(x+2, y)=P_2$ übergeführt. Die Operatoren $a^2 b^2$, $(a^2 b^2)^2$, $(a^2 b^2)^3$, ... geben demnach eine Reihe von Punkten, die auf einer Parallelen zur X-Achse liegen und die Abszissen $x+2, x+4, x+6, \ldots$ haben. Daraus ist ersichtlich, daß die Ordnung von $a^2 b^2$ nicht endlich sein kann. Ebenso erkennt man leicht, daß $b^2 a^2$ den Punkt P in $P_3=(x-2, y)$ überführt, so daß auch $b^2 a^2$ ein Operator von unendlich großer Ordnung wird.

---

3. Kapitel.

Teiler einer Gruppe. Isomorphismus.

§ 22. Wir haben (§ 16, S. 20) durch das Symbol

(1) $$C = [a, b, c, \ldots, f, g]$$

den Komplex C der in die eckige Klammer eingeschlossenen Operatoren bezeichnet, gleichgültig, ob ihm die Gruppeneigenschaften zukommen oder nicht.

Unter dem Symbole

(2) $$G = \{a, b, c, \ldots, f, g\}$$

verstehen wir dagegen die Gruppe niedrigster Ordnung, die die Operatoren $a, b, c, \ldots, f, g$ enthält, ohne daß freilich durch (2) die Existenz einer endlichen Gruppe verbürgt wäre. Im allgemeinen wird (2) mehr als die angegebenen, in die Klammer geschlossenen Operatoren enthalten. So ist z. B.

$$\{a\} = [1, a, a^2, \ldots, a^{n-1}],$$

wenn n die Ordnung des Operators a angibt, eine zyklische Gruppe der Ordnung n.

Ähnlich soll unter dem Symbole

(3) $$\{G, H, K, \ldots\},$$

in dem $G, H, K, \ldots$ Gruppen bedeuten, die Gruppe verstanden werden, die die einzelnen Gruppen $G, H, K, \ldots$ enthält und dabei von niedrigster Ordnung ist. (3) möge gesprochen werden: „Multiplum von $G, H, K, \ldots$"; es ist (3) gewissermaßen das kleinste gemeinsame Vielfache von $G, H, K, \ldots$

Bedeuten C_1 und C_2 zwei Komplexe von Operatoren

$$C_1 = [a, b, c, \ldots]; \quad C_2 = [\alpha, \beta, \gamma, \ldots],$$

so soll $C_1 \cdot C_2$ den Komplex aller Produkte $a\alpha, a\beta, a\gamma, \ldots, b\alpha, b\beta, b\gamma, \ldots, c\alpha, c\beta, c\gamma, \ldots$ bedeuten. Von $C_1 \cdot C_2$ ist $C_2 \cdot C_1$ im allgemeinen verschieden. — Die Gleichung

(4) $$C \cdot C = C$$

ist mit der Bedingung I aus § 1 identisch, denn sie sagt

aus, daß das Kompositionsresultat zweier Operatoren aus C wieder in C enthalten ist.

Alle Operatoren, die in zwei oder mehreren Gruppen $G, H, K, \ldots$ gleichzeitig enthalten sind, bilden eine Gruppe M. Denn kommen die Operatoren a und b in $G, H, K, \ldots$ vor, so auch $a \cdot b$. Diese Gruppe M heißt der größte gemeinsame Teiler von $G, H, K, \ldots$; wir bezeichnen ihn durch

$$(5) \quad M = \text{Div}(G, H, K, \ldots) \quad \text{oder} \quad M = \} G, H, K, \ldots \{ .$$

(5) möge gesprochen werden: „Divisor von $G, H, K, \ldots$"

§ 23. Sind alle Operatoren einer Gruppe H auch in der Gruppe G enthalten, so heißt H ein Teiler, ein Divisor oder eine Untergruppe von G, und G ein Multiplum oder ein Vielfaches von H. Enthält H nicht alle Operatoren von G, so ist es ein echter oder eigentlicher Teiler von G; stimmen H und G überein, so ist H ein unechter oder uneigentlicher Teiler von G. Ist $\text{Div}(G, H) = 1$, so heißen G und H teilerfremd.

H ist ein Teiler von G, wenn

$$G = \{G, H\} \quad \text{oder wenn} \quad H = \} G, H \{ .$$

Ist a ein Operator von G, so ist $\{a\}$ ein Teiler von G, aber nicht notwendig ein echter; sind a und b Operatoren von G, so ist $\{a, b\}$ ein Teiler von G.

Nun möge H ein eigentlicher Teiler von G sein, r bezeichne seine Ordnung und $1, a_2, a_3, \ldots, a_{r-1}, a_r$ seine sämtlichen Operatoren; dann wird

$$(6) \qquad H = [1, a_2, a_3, \ldots, a_{r-1}, a_r] .$$

Da H ein eigentlicher Teiler von G ist, so gibt es in G einen Operator b_2, der in H nicht vorkommt. Dann enthält G auch alle Produkte, die im Komplexe

$$(7) \qquad b_2 H = [b_2, b_2 a_2, b_2 a_3, \ldots, b_2 a_{r-1}, b_2 a_r]$$

auftreten. Alle Operatoren von (7) sind unter sich und von den Operatoren (6) verschieden. Denn aus der Gleichung $b_2 a_\alpha = b_2 a_\gamma$ würde nach II, § 1 folgen $a_\alpha = a_\gamma$. Und aus $b_2 a_\alpha = a_\delta$ ergäbe sich $b_2 = a_\delta a_\alpha^{-1} = a_\varepsilon$, d. h. b_2 käme gegen die Annahme schon in H vor.

Die Gruppe G enthält daher mindestens die $2r$ untereinander verschiedenen Operatoren (6) und (7). Erschöpfen diese die Gruppe G noch nicht, so gibt es einen neuen, weder in (6) noch in (7) vorkommenden Operator b_3 von G. Mit ihm bilden wir den Komplex

$$(8) \qquad b_3 H = [b_3 \, , \; b_3 a_2 \, , \; b_3 a_3 \, , \; \ldots , \; b_3 a_{r-1} \, , \; b_3 a_r]$$

und zeigen wie oben, daß alle seine Elemente unter sich und von den Operatoren (6) und (7) verschieden sind. Danach enthält G mindestens $3r$ Operatoren.

Fährt man in gleicher Art fort, so erschöpft man schließlich die Operatoren der endlichen Gruppe G. Der letzte dabei auftretende Komplex mag

$$(9) \qquad b_t H = [b_t \, , \; b_t a_2 \, , \; b_t a_3 \, , \; \ldots , \; b_t a_{r-1} \, , \; b_t a_r]$$

sein. Dann folgt für die Ordnung n der Gruppe G die Gleichung $n = r \cdot t$. Somit ersieht man: Ist die Gruppe H der Ordnung r ein eigentlicher Teiler der Gruppe G, so ist die Ordnung n von G ein eigentliches Vielfaches von r. Den Quotienten $n : r = t$ nennen wir den Index des Teilers H von G. Natürlich kann H auch $= \{a\}$ sein, wenn a ein Operator von G ist. Daher gilt: Die Ordnung einer Gruppe G ist ein Vielfaches der Ordnung jedes ihrer Operatoren. Hiermit ist der in § 17, S. 24 benutzte Satz hergeleitet.

§ 24. Im vorigen Paragraphen gingen wir von der Gruppe H aus und bildeten mit Hilfe neuer Operatoren b_2, b_3, ..., b_t gewisse Komplexe (7), (8), (9), ... Wir wollen sie die Nebenkomplexe zu H in G nennen und schreiben

$$(10) \qquad G = H + b_2 H + b_3 H + \ldots + b_t H \, .$$

Hierbei sind die $+$Zeichen nur dazu bestimmt, die Zusammenfassung der in den einzelnen Summanden auftretenden Operatoren anzudeuten.

Wir bemerken, daß die b_2, b_3, ..., b_t nicht eindeutig bestimmt sind; denn der Operator b_α kann durch jedes Produkt $b_\alpha a_\varkappa$ ($\varkappa = 1, 2, \ldots r$) ersetzt werden, da $(b_\alpha a_\varkappa) H = b_\alpha (a_\varkappa H) = b_\alpha H$ ist. Dagegen sind die Nebenkomplexe in (10), abgesehen von ihrer Anordnung, vollkommen durch G und H bestimmt. Denn hätte man

z. B. auch die Zerlegung von G in Nebenkomplexe von der Form

(10a) $$G = H + d_2 H + d_3 H + \dots + d_t H \,,$$

so müßte ein Operator des Komplexes $d_\alpha H$ in einem der Komplexe (10), z. B. in $b_\beta H$, vorkommen, d. h. es wäre für passend gewählte Indizes ϱ und σ

$$d_\alpha a_\varrho = b_\beta a_\sigma \,;$$

daraus folgte aber

$$d_\alpha = b_\beta a_\sigma a_\varrho^{-1} = b_\beta a_\tau \,,$$

$$d_\alpha H = b_\beta a_\tau H = b_\beta H \,,$$

d. h. die Komplexe $d_\alpha H$ und $b_\beta H$ stimmten dann völlig überein. —

Genau in der gleichen Weise, wie wir bei der Komposition in (7) den Operator b_2 als linksseitigen Faktor von H genommen haben, hätten wir auch b_2 zum rechtsseitigen Faktor nehmen können. Führen wir dies durch, indem wir die neu hinzutretenden Operatoren mit $b_2 = c_2$, c_3, ..., c_t bezeichnen, so erhalten wir die zweite Zerlegung von G in H und seine Nebenkomplexe

(10b) $$G = H + H c_2 + H c_3 + \dots + H c_t \,.$$

Daß für die Anzahl der Summanden wieder t genommen werden mußte, wie bei (10), ist klar.

Man erkennt leicht, daß die Summanden von (10) im allgemeinen nicht denen von (10b) gleich sind. Am einfachsten zeigt dies ein Beispiel. Wir wählen (5) in § 17, S. 27 und setzen $H = [1, b]$. Dann liefert (10) die Komplexzerlegung

$$G = [1,\ b] + [a\,,\ a\,b] + [a^2,\ a^2 b] \,,$$

dagegen (10b) die folgende

$$G = [1,\ b] + [a\,,\ b\,a] + [a^2,\ b\,a^2] \,,$$

von der ersten verschiedene, wobei

$$[a\,,\ b\,a] = [a\,,\ a^2 b] \,, \quad [a^2,\ b\,a^2] = [a^2,\ a\,b] \,.$$

Wir weisen gleich hier darauf hin, daß der Fall der Übereinstimmung der beiden Zerlegungen (10) und (10b) von besonderer Wichtigkeit ist.

§ 25. Von dem fundamentalen Satze des § 23 wollen wir jetzt einige Anwendungen machen. Wir sahen schon: Ist a ein Operator der Gruppe G, so ist die Ordnung von a ein Teiler der Ordnung von G. Es enthält nämlich G mit a zugleich die Gruppe $H = \{a\}$, wie das ja bereits bemerkt wurde.

Aus diesem Satze ergibt sich sofort: Die Ordnung einer Gruppe ist ein Vielfaches des kleinsten gemeinsamen Vielfachen der Ordnungen aller ihrer Operatoren.

Wir besprechen nunmehr einige Anwendungen der hergeleiteten Sätze auf die Substitutionengruppen.

Jede Substitutionengruppe G ist ein Teiler der symmetrischen Gruppe S aller ihrer Elemente. Ist ihre Anzahl $= n$, so wird nach § 6 die Ordnung von S gleich $n!$ Demnach kann die Ordnung r der Substitutionengruppe G nur ein Teiler von $n!$ sein. Den Index $n!:r$ nennen wir den Index der Substitutionengruppe G (in bezug auf die symmetrische Gruppe S); dieser Index ist der zu r komplementäre Teiler von $n!$ Diese Betrachtungen zeigen, daß von den als Ordnungen einer Substitutionengruppe des Grades n denkbaren Zahlen eine ganze Reihe ausgeschaltet werden muß. Ist $n = 3$, so kann r nur $= 1, 2, 3$ oder 6 sein; $r = 4$ und $r = 5$ ist dagegen unmöglich. Jene vier Zahlen $1, 2, 3, 6$ kommen auch wirklich als Ordnungen von Substitutionengruppen dreier Elemente vor. Bezeichnen wir nämlich die drei Elemente mit a, b, c und mit 1 die Einheitssubstitution, so entsprechen sie als Ordnungszahlen den Gruppen

(I) 1.

(II) $1, (a\,b)$.

(III) $1, (a\,b\,c), (a\,c\,b)$.

(IV) $1, (a\,b), (a\,c), (b\,c), (a\,b\,c), (a\,c\,b)$.

Ist $n = 4$, so darf r nur einen der Werte $1, 2, 3, 4, 6, 8, 12, 24$ annehmen; die übrigen 16 Werte $5, 7, 9, 11, \ldots 21, 22, 23$ müssen ausgeschlossen werden. Für die angegebenen acht möglichen Fälle bestehen auch wirklich Substitutionengruppen. Für $r = 1, 2, 3, 6$ können wir die Gruppen der soeben aufgestellten Tabelle nehmen;

daß nur drei Elemente in die Zyklen explizit eingehen, ist offenbar gleichgültig; wir können jeder Substitution den Zykel (d) hinzufügen. Für die weiteren Werte von r hat man

(V) $\quad 1,\ (a\,b\,c\,d),\ (a\,c)\,(b\,d),\ (a\,d\,c\,b)$.

(VI) $\quad 1,\ (a\,b\,c\,d),\ (a\,c)\,(b\,d),\ (a\,d\,c\,b),\ (a\,c),\ (b\,d),$
$(a\,b)\,(c\,d),\ (a\,d)\,(b\,c)$.

(VII) $\quad 1,\ (a\,b)\,(c\,d),\ (a\,c)\,(b\,d),\ (a\,d)\,(b\,c),\ (a\,b\,c),\ (a\,c\,b),$
$(a\,b\,d),\ (a\,d\,b),\ (a\,c\,d),\ (a\,d\,c),\ (b\,c\,d),\ (b\,d\,c)$.

(VII) ist die alternierende Gruppe der vier Elemente a, b, c, d. Zu $r = 24$ gehört die symmetrische Gruppe. Allgemein gibt es für jedes n eine Gruppe der Ordnung $r = \frac{1}{2}n!$, nämlich die alternierende, ihr Index ist gleich 2, und eine der Ordnung $n!$, nämlich die symmetrische.

Es möge darauf hingewiesen werden, daß für gleiche n und r mehrere, ihrem Typus nach verschiedene Gruppen bestehen können. So kann z. B. statt (II) auch

$$G = [1,\ (a\,b)\,(c\,d)]$$

genommen werden und statt (V) auch die Vierergruppe

$$G = [1,\ (a\,b)\,(c\,d),\ (a\,c)\,(b\,d),\ (a\,d)\,(b\,c)]\ .$$

In den besprochenen Fällen gehört zu jedem Teiler r von $n!$ eine Gruppe. Das gilt nicht allgemein. Schon bei $n = 5$ gibt es keine Substitutionengruppen von einer der Ordnungen 30 oder 40, d. h. vom Index 4 oder 3, trotzdem diese Zahlen Teiler von $n! = 120$ sind.

§ 26. Wir wollen nachweisen, daß unter allen Substitutionengruppen die alternierenden die einzigen sind, die den Index 2 haben.

Ist G eine Gruppe vom Index 2, die nicht mit der alternierenden identisch ist, so gibt es nach § 11, S. 14 zyklische Substitutionen dritter Ordnung, die nicht in G vorkommen; t sei eine solche. Nun bilden wir die zu G gehörigen Nebenkomplexe, die die Zerlegung der symmetrischen Gruppe S liefern. Wir können sie

$$S = G + tG + t^2G + \dots$$

bezeichnen. Denn $t^2 G$ muß von G und $t G$ verschieden sein, da aus einer der Gleichungen

$$t^2 G = G \quad \text{oder} \quad t^2 G = t G$$

folgen würde, daß t^2 oder t schon zu G gehörte. Das zweite ist durch die Annahme über t ausgeschlossen; das erste dadurch, daß sonst mit t^2 auch $(t^2)^2 = t$ in G vorkäme. Die obige Zerlegung zeigt nun, daß dann G mindestens den Index 3 haben muß.

Genau nach der gleichen Methode kann man den folgenden Satz herleiten: Ist G eine abstrakte Gruppe, H ein eigentlicher Teiler von G und q ein Operator der Primzahlordnung $\varkappa$, der in G, aber nicht in H vorkommt, so ist der Index des Teilers H von G mindestens gleich $\varkappa$. Es zeigt sich nämlich bei der Herstellung der Nebenkomplexe zu H in G, daß die Zerlegung auf

$$G = H + qH + q^2 H + \ldots + q^{\varkappa - 1} H + \ldots$$

führt, da alle Operatoren in H, qH, $q^2 H$, $\ldots$, $q^{\varkappa - 1} H$ voneinander verschieden sind, sobald q von einer Primzahlordnung ist.

§ 27. Wir kommen jetzt zur Einführung eines neuen, wichtigen Begriffes.

Es mögen zwei Substitutionengruppen von gleicher Ordnung r gegeben sein,

$$G = [1,\ a_2,\ a_3,\ \ldots,\ a_{r-1},\ a_r],$$
$$\Gamma = [1,\ \alpha_2,\ \alpha_3,\ \ldots,\ \alpha_{r-1},\ \alpha_r],$$

und es sei möglich, ihre einzelnen Substitutionen a_ϱ und α_ϱ einander paarweise so zuzuordnen, daß dem Produkte $a_\varrho a_\sigma$ zweier Substitutionen aus G das Produkt $\alpha_\varrho \alpha_\sigma$ der zugeordneten aus Γ wieder zugeordnet ist: dann nennen wir G und Γ einstufig isomorph oder kürzer isomorph; wir sagen: G und Γ stehen in einstufigem Isomorphismus zueinander. Als Beispiel mögen G und Γ mit den Substitutionen aus drei und aus sechs Elementen

$$1,\ a_2 = (123),\ a_3 = (132),\ a_4 = (12),\ a_5 = (13),\ a_6 = (23)$$

und

$$1,\ \alpha_2 = (132)(456),\ \alpha_3 = (123)(465),\ \alpha_4 = (14)(25)(36),$$
$$\alpha_5 = (15)(26)(34),\ \alpha_6 = (16)(24)(35)$$

dienen, bei denen man $a_\varkappa$ und $\alpha_\varkappa$ einander zuordnet. In der Tat gelten dann z. B. die Gleichungspaare

$$a_2^2 = a_3\,,\ \alpha_2^2 = \alpha_3\,;\quad a_2\,a_4 = a_6\,,\ \alpha_2\,\alpha_4 = \alpha_6\,;$$
$$a_5\,a_6 = a_2\,,\ \alpha_5\,\alpha_6 = \alpha_2\,;\ \text{usw.}$$

Aus der Vergleichung der Kompositionsformeln, nach denen gleichzeitig

$$a_\varrho\,a_\sigma = a_\tau \quad \text{und} \quad \alpha_\varrho\,\alpha_\sigma = \alpha_\tau$$

wird, können wir den Schluß ziehen, daß einstufig isomorphe Gruppen, von der Bezeichnung abgesehen, die gleiche Cayleysche Tabelle ergeben. Für unser Beispiel wird sie bei beiden Gruppen dem Quadrate

	q_1	q_2	q_3	q_4	q_5	q_6
q_1	q_1	q_2	q_3	q_4	q_5	q_6
q_2	q_2	q_3	q_1	q_6	q_4	q_5
q_3	q_3	q_1	q_2	q_5	q_6	q_4
q_4	q_4	q_5	q_6	q_1	q_2	q_3
q_5	q_5	q_6	q_4	q_3	q_1	q_2
q_6	q_6	q_4	q_5	q_2	q_3	q_1

gleich, falls jedes q_ϱ durch a_ϱ oder α_ϱ ersetzt wird. Dieses Quadrat ist mit (5), § 17, S. 27 identisch, wenn man die Reihen umstellt und setzt, was erlaubt ist,

$$q_1 = 1\,,\quad q_2 = a\,,\quad q_3 = a^2,\quad q_4 = a\,b\,,\quad q_5 = b\,,\quad q_6 = a^2 b\,.$$

Der Begriff des einstufigen Isomorphismus fällt demnach bei abstrakten Gruppen mit dem der Identität zusammen, da ja zwei einstufig isomorphe, abstrakte Gruppen bis auf die Bezeichnung einander gleich sind.

Als ein zweites Beispiel führen wir das folgende an: die Gruppe des Grades 8

$$a_1 = 1\,,\quad a_2 = (12)\,(34)\,(58)\,(67)\,,\quad a_3 = (13)\,(24)\,(57)\,(68)\,,$$
$$a_4 = (14)\,(23)\,(56)\,(78)\,,\quad a_5 = (15)\,(27)\,(38)\,(46)\,,$$
$$a_6 = (16)\,(28)\,(37)\,(45)\,,\quad a_7 = (1847)\,(2635)\,,$$
$$a_8 = (1748)\,(2536)$$

und die Gruppe vom Grade 4

$$\alpha_1 = 1\,,\quad \alpha_2 = (13)\,,\quad \alpha_3 = (24)\,,\quad \alpha_4 = (13)\,(24)\,,$$

$$\alpha_5 = (14)\,(23)\,,\quad \alpha_6 = (12)\,(34)\,,\quad \alpha_7 = (1432)\,,\quad \alpha_8 = (1234)\,,$$

wobei die a_ϱ den α_ϱ entsprechen, sind isomorph.

Die beiden Substitutionengruppen G und Γ erscheinen in ihrer Darstellung voneinander wesentlich verschieden; in ihrem Aufbau dagegen wesentlich gleich. Dies wird noch deutlicher, wenn man von G und von Γ zu den abstrakten, ihnen entsprechenden Gruppen gemäß den Vorschriften des § 16 übergeht. Die dort hergeleiteten Resultate zeigen in Verbindung mit den Entwicklungen dieses Paragraphen: Jeder Substitutionengruppe, die nicht selbst regulär ist, ist eine reguläre einstufig isomorph.

Von einstufig isomorphen Gruppen sagen wir, sie besitzen gleichen Typus oder gleiche Konstitution, d. h. sie haben dieselben Kompositionsvorschriften. Offenbar gilt der Satz: Operatoren, die sich isomorph entsprechen, haben gleiche Ordnungen.

§ 28. Eine Substitutionengruppe kann auch auf sich selbst einstufig isomorph bezogen sein, und wir werden im nächsten Kapitel ein Verfahren kennen lernen, durch das im allgemeinen ein solcher Isomorphismus festgelegt werden kann. Wir wählen hier als Beispiel solcher Beziehungen die symmetrische Substitutionengruppe von drei Elementen, die wir mit 1, 2, 3 bezeichnen,

(I) 1, (12), (13), (23), (123), (132).

Der identischen Substitution 1 muß stets die gleiche 1 zugeordnet sein.

Die drei Transpositionen (12), (13), (23) müssen bei jedem Isomorphismus sich untereinander entsprechen. Durch die Festsetzung dieses Entsprechens ist das der letzten zwei Zyklen dritter Ordnung festgelegt. Es gibt also nur die folgenden fünf Zuordnungen, bei denen die Operatoren an gleichen Stellen sich entsprechen, und es bestehen ebenso viele isomorphe Beziehungen zur Gruppe (I), von der wir ausgingen:

(II) 1, (12), (23), (13), (132), (123);

(III) 1, (23), (13), (12), (132), (123);

(IV) 1, (13), (12), (23), (132), (123);

(V) 1, (13), (23), (12), (123), (132);

(VI) 1, (23), (12), (13), (123), (132).

§ 29. Wir erweitern den Begriff des Isomorphismus in folgender Art: Zwischen den Operatoren α, β, γ, δ, ... der Gruppe Γ und den Operatoren a, b, c, d, ... der Gruppe G mögen folgende Beziehungen stattfinden: Jedem Operator von Γ lassen sich s Operatoren von G zuordnen, etwa dem Operator

α aus Γ die Operatoren $a_1, a_2, a_3, \ldots, a_s$ aus G,
β aus Γ die Operatoren $b_1, b_2, b_3, \ldots, b_s$ aus G,
γ aus Γ die Operatoren $c_1, c_2, c_3, \ldots, c_s$ aus G, usw.

derart, daß dem Produkte zweier Operatoren $\alpha \cdot \beta$ aus Γ jedes Produkt $a_\sigma \cdot b_\tau$ zweier ihnen bzw. zugeordneter Operatoren entspricht, also wenn $\alpha \cdot \beta = \gamma$ ist, daß der Komplex

$$[a_\sigma b_\tau] = [c_v] \qquad (\sigma, \tau, v = 1, 2, 3, \ldots, s)$$

wird. Finden diese Beziehungen zwischen G und Γ statt, so sagen wir, G stehe in s-stufigem Isomorphismus zu Γ, oder G sei s-stufig isomorph zu Γ.

Beispielsweise ist die oben in § 14 aufgestellte Gruppe

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*
a	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*
b	*b*	*a*	*d*	*c*	*h*	*g*	*f*	*e*
c	*c*	*d*	*a*	*b*	*g*	*h*	*e*	*f*
d	*d*	*c*	*b*	*a*	*f*	*e*	*h*	*g*
e	*e*	*g*	*h*	*f*	*a*	*d*	*b*	*c*
f	*f*	*h*	*g*	*e*	*d*	*a*	*c*	*b*
g	*g*	*e*	*f*	*h*	*c*	*b*	*d*	*a*
h	*h*	*f*	*e*	*g*	*b*	*c*	*a*	*d*

zu

	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	α	β
δ	δ	γ	β	α

zweistufig isomorph, falls man den Operatoren

$$\alpha; \; \beta; \; \gamma; \; \delta$$

aus Γ entsprechend je die beiden Operatoren aus G

$$a, d; \quad b, c; \quad g, h; \quad e, f$$

zuordnet. Denn dabei wird z. B. dem $\delta\beta = \gamma$ das g oder das h zugeordnet. Die a und α sind die Einheitsoperatoren der beiden Gruppen, da $a^2 = a$; $\alpha^2 = \alpha$ ist.

Die gleiche Gruppe G von achter Ordnung wird vierstufig isomorph zu der Gruppe

	α	β
α	α	β
β	β	α ,

indem man den Operatoren

$$\alpha\,;\ \beta$$

aus Γ entsprechend je vier aus G, nämlich bzw.

$$a\,,\ d\,,\ g\,,\ h\,;\quad b\,,\ c\,,\ e\,,\ f$$

zuordnet. Dabei entsprechen beispielsweise dem Produkte $\beta \cdot \beta = \alpha$ die 16 Produkte

$b \cdot b = a$, $b \cdot c = d$, $b \cdot e = h$, $b \cdot f = g$, $c \cdot b = d$, $c \cdot c = a$ usw.,

die sich auf die vier verschiedenen a, d, g, h reduzieren.

Die in § 28 aufgestellte Gruppe (I) von sechster Ordnung ist zu der Gruppe zweiter Ordnung

$$\Gamma = [1\,,\ (\alpha\,\beta)]$$

dreistufig isomorph, wenn man der Einheit in Γ aus G die drei Substitutionen

$$1,\ (123)\,,\ (132)$$

zuordnet und der Substitution $(\alpha\,\beta)$ die drei anderen Substitutionen aus G, die noch zurückbleiben,

$$(12)\,,\ (13)\,,\ (23)\,.$$

§ 30. Die abstrakte Gruppe G stehe zu der abstrakten Gruppe Γ in s-stufigem Isomorphismus. Dann bilden die s Operatoren von G, die dem Einheitsoperator in Γ zugeordnet sind, einen Teiler von G. Denn sind a und b zwei Operatoren von G, die beide der Einheit in Γ entsprechen, so entspricht $a \cdot b$ dem Produkte $1 \cdot 1 = 1$, d. h. $a \cdot b$ entspricht auch der Einheit und gehört also zu dem Kom-

plexe, dem schon a und b angehören. Demnach bilden die $a, b, \ldots$ eine Gruppe E der Ordnung s, die ein Teiler von G ist.

Nun nehmen wir einen beliebigen Operator a aus G und den entsprechenden α aus Γ; die Produkte $a \cdot E$, d. h. der Komplex der Produkte aus a und je einem Operator aus E, liefern alle dem α entsprechenden Operatoren aus G. Denn jeder Operator aus $a \cdot E$ entspricht dem $\alpha \cdot 1 = \alpha$; und umgekehrt, wenn a und a_1 dem α entsprechen, so entspricht $a_1 \cdot a^{-1}$ dem $\alpha \cdot \alpha^{-1} = 1$, d. h. $a_1 \cdot a^{-1}$ gehört zu E und a_1 zu $aE = Ea$.

Dem Operator α aus Γ entspreche a aus G; dann entspricht jedes α^ϱ dem a^ϱ für alle Exponenten $\varrho = 1, 2, 3, \ldots$ Nimmt man für ϱ die niedrigste Zahl μ, für die a^μ zu E gehört, so wird $\alpha^\mu = 1$ (μ, min), und a^μ, $a^{2\mu}$, $a^{3\mu}, \ldots$ sind die einzigen Potenzen von a, die in E vorkommen. Also ist die Ordnung von a gleich einem Produkte $\mu \cdot \nu$, und die von α ist ein Teiler μ von $\mu \cdot \nu$. Aus $(a^\mu)^\nu = 1$ erkennt man, daß ν ein Teiler der Ordnung s von E wird. Hat α die Ordnung μ, so hat a die Ordnung $\mu\nu$, wobei ν ein Teiler der Ordnung s von E ist. Ist die Ordnung von a, d. h. ist $\mu \cdot \nu$ teilerfremd zu der Ordnung von E, so haben a und α gleiche Ordnungen, da $\nu = 1$ wird.

In dem ersten Beispiele aus § 29 haben β und b sowie c die gleiche Ordnung, nämlich 2; dagegen hat γ die Ordnung 2, und g sowie h besitzen die Ordnung 4; ferner sind δ, e und f wieder von der Ordnung 2.

Es läßt sich leicht beweisen: Jedem Teiler H von Γ entspricht ein Teiler H von G. Der Index von H in bezug auf Γ ist dem von H in bezug auf G gleich, und die Ordnung von H ist demnach das s-fache der Ordnung von H. Dabei besteht H aus den Komplexen der Operatoren, die den einzelnen, in H vorkommenden Operatoren von G zugeordnet sind.

Die Umkehrung dieses Satzes ist, wie wir sehen werden, gewissen Einschränkungen unterworfen.

Gegeben sei ein Teiler H der Ordnung r von G; gesucht wird der Teiler H von Γ, der aus allen den Operatoren von Γ besteht, die denen von H entsprechen. — Es sei $E' = \}H, E\{$ von der Ordnung s'. Die Gruppe E'

ist ein Teiler von Π; seine Nebenkomplexe in H sind durch die Zerlegung des gegebenen Teilers H bestimmt:

$$H = E' + t_2 E' + t_3 E' + \dots + t_\varrho E' \qquad (r = \varrho \cdot s').$$

Nun sollen t_α und t_β Operatoren der Reihe $t_2, t_3, \dots, t_\varrho$ bezeichnen. Dem Operator t_α entspreche in Γ der Operator τ_α. Da E' ein Teiler von E ist, und da allen Operatoren von E in Γ die Einheit entspricht, so ist allen Operatoren des Komplexes $t_\alpha E'$ der eine Operator τ_α zugeordnet. Ferner entsprechen zwei verschiedenen t_α, t_β auch verschiedene τ_α, τ_β; denn aus der Gleichung $\tau_\beta = \tau_\alpha$ müßte folgen: t_β gehört zu $t_\alpha E$; also, da t_β und t_α zu H gehören, t_β kommt in $t_\alpha E'$ vor, was ausgeschlossen ist. Demnach ist die Ordnung des Teilers H von Γ, der dem Teiler H von G entspricht, gleich ϱ, d. h. gleich $r:s'$. Ist H Teiler der Ordnung r einer Gruppe G, die s-stufig isomorph zu Γ ist, so entspricht dem H ein Teiler H der Gruppe Γ von der Ordnung $\varrho = r:s'$. Dabei bedeutet s' die Ordnung von $\}H, E\{$. Enthält H den Teiler E, so wird $\varrho = r:s$; sind H und E teilerfremd, so besitzen H und H gleiche Ordnungen.

Als Beispiel für diese Verhältnisse diene das Folgende. Die linksstehende Gruppe achter Ordnung ist bei der angedeuteten Zuordnung zweistufig isomorph zu der rechtsstehenden vierter Ordnung

1,	(12) (34)	1;
(13) (24),	(14) (23)	$(a\,b)\,(c\,d)$;
(1324),	(1423)	$(a\,c)\,(b\,d)$;
(12),	(34)	$(a\,d)\,(b\,c)$.

Hier entspricht nun jeder der beiden Gruppen H und H_1, welche Teiler der linksstehenden Gruppe sind,

$$H = [1,\ (12)\,(34),\ (13)\,(24),\ (14)\,(23)],$$

$$H_1 = [1,\ (13)\,(24)],$$

dieselbe Gruppe

$$\mathsf{H} = [1,\ (a\,b)\,(c\,d)],$$

trotzdem H und H_1 von verschiedenen Ordnungen sind.

4. Kapitel.

Transformation und Vertauschbarkeit.

§ 31. Den mit Hilfe zweier Operatoren a und b gebildeten neuen Operator $a^{-1}ba$ nennt man die Transformierte von b durch a. Man sieht leicht: Die Transformierte eines Produktes $b \cdot c$ ist gleich dem Produkte der Transformierten seiner Faktoren b und c. Denn es ist ja

(1) $$a^{-1}(b\,c)\,a = a^{-1}\,b\,(a \cdot a^{-1})\,c\,a = (a^{-1}\,b\,a)\,(a^{-1}\,c\,a)\,.$$

Folglich ist auch für Potenzierungen bei beliebigem Exponenten μ

(2) $$(a^{-1}\,b\,a)^{\mu} = a^{-1}\,b^{\mu}\,a\,.$$

Ist d die Transformierte von b durch a, so ist b die Transformierte von d durch a^{-1}; denn aus $a^{-1}\,b\,a = d$ folgt $b = a\,d\,a^{-1} = (a^{-1})^{-1}\,d(a^{-1})$.

Transformierte Operatoren b und $a^{-1}ba$ haben gleiche Ordnungen. Dies folgt aus der Gleichung (2):

$$(a^{-1}\,b\,a)^{\mu} = a^{-1}\,b^{\mu}\,a\,.$$

Denn ist μ die Ordnung von b, dann folgt $(a^{-1}\,b\,a)^{\mu} = 1$; also ist die Ordnung von $a^{-1}\,b\,a$ ein echter oder unechter Teiler der Ordnung von b; bedeutet dagegen μ die Ordnung von $a^{-1}\,b\,a$, dann ist $a^{-1}\,b^{\mu}\,a = 1$, $b^{\mu} = a^{+1} \cdot a^{-1} = 1$, und das zeigt, daß die Ordnung von b ein echter oder unechter Teiler der Ordnung von $a^{-1}\,b\,a$ ist. Folglich stimmen beide Ordnungen überein.

Die Transformierten zweier Reziproken sind selbst reziprok. Denn aus $c = b^{-1}$ folgt (§ 6; S. 7)

$$a^{-1}\,c\,a = a^{-1}\,b^{-1}\,a = (a^{-1}\,b\,a)^{-1}.$$

Aus (1) folgt ferner: Transformiert man die Operatoren einer Gruppe G sämtlich durch den gleichen Operator a, so entsteht eine Gruppe G_1, die zu G einstufig isomorph ist, falls man transformierte Operatoren einander zuordnet, $G_1 = a^{-1}\,G\,a$.

Ist der Operator a, durch den man transformiert, ein zu G selbst gehöriger Operator, so wird $G_1 = G$, und

G erscheint durch diese Transformation als einstufig isomorph auf sich selbst bezogen. So entstehen z. B. die sechs isomorphen Gruppen in § 28 aus der ersten unter ihnen durch Transformation mit bzw. 1; (23); (13); (12); (132); (123).

§ 32. Wir wollen den neu eingeführten Begriff der Transformation an den Substitutionen und an den Substitutionengruppen näher erläutern.

Es seien

$$s = \binom{a_\varkappa}{a_{i_\varkappa}}, \quad t = \binom{a_\varkappa}{b_\varkappa} \qquad (\varkappa = 1, 2, 3, \ldots, n)$$

zwei Substitutionen, in denen die $a_\varkappa$ und die $a_{i_\varkappa}$ die Reihe der Elemente $a_1, a_2, \ldots, a_n$ durchlaufen, während die $b_\varkappa$ willkürliche, mit den a_λ übereinstimmende oder von ihnen verschiedene Elemente sein sollen. Dann wird die Transformierte von s durch t

$$t^{-1} s\, t = \binom{b_\varkappa}{a_\varkappa}\binom{a_\varkappa}{a_{i_\varkappa}}\binom{a_\varkappa}{b_\varkappa} = \binom{b_\varkappa}{a_{i_\varkappa}}\binom{a_{i_\varkappa}}{b_{i_\varkappa}} = \binom{b_\varkappa}{b_{i_\varkappa}};$$

d. h. man erhält die Transformierte von s durch t, indem man auf die Elemente von s die Substitution t ausführt, d. h. jedes $a_\varkappa$ durch $b_\varkappa$ ersetzt. Jedem Zykel in s entspricht daher in $t^{-1} s\, t$ ein Zykel von gleicher Elementenanzahl, d. h. von gleicher Ordnung; und $t^{-1} s\, t$ besteht aus ebenso vielen Zyklen von entsprechend gleicher Ordnung wie s. Deshalb heißen auch die Substitutionen s und $t^{-1} s\, t$ einander ähnlich oder auch von gleichem Typus.

Setzen wir z. B.

$$s = (12)\,(345)\,(6789)\,, \quad t = (03)\,(197)\,(24)\,(685)\,,$$

so wird

$$\begin{aligned} t^{-1} s\, t &= (03)(179)(24)(658)\cdot(12)(345)(6789)\cdot(03)(197)(24)(685) \\ &= (026)(1578)(3)(49) = (49)(026)(1578)\,. \end{aligned}$$

Das Resultat ist demnach dasselbe, als ob man auf die Elemente von s die durch

$$t = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 4 & 0 & 2 & 6 & 8 & 1 & 5 & 7 \end{pmatrix}$$

vorgeschriebene Umstellung gemacht hätte.

Ist eine Substitution s_1 einer anderen s ähnlich, so kann man jede von ihnen aus der anderen mittels Transformation durch eine passend gewählte dritte t herleiten. Um eine solche zu finden, genügt es, s und s_1 so untereinander zu schreiben, daß Zyklen von gleicher Ordnung, die aber sonst beliebig gewählt sein können, untereinander stehen; die Anfangsglieder der Zyklen sind dabei nicht fest bestimmt (§ 7). Dann unterdrückt man die Klammern, die die Zyklen umfassen, schließt beide Zeilen in eine neue Klammer ein und faßt das Entstehende als Ausdruck einer Substitution auf (§ 5).

So findet man für die beiden einander ähnlichen Substitutionen

$$s = (12)\,(34)\,(567)\,, \quad s_1 = (15)\,(28)\,(346)$$

unter anderen für t die Formen

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\1&5&2&8&3&4&6&7\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5&6&7&8\\5&1&8&2&6&3&4&7\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5&6&7&8\\2&8&1&5&4&6&3&7\end{pmatrix}.$$

§ 33. Bedeuten s und t zwei ganz beliebige Substitutionen, so sind st und ts einander ähnliche Substitutionen; denn wegen der Gleichungen

$$t^{-1}(ts)\,t = st\,, \quad s^{-1}(st)\,s = ts$$

ist jede eine Transformierte der andern. Also haben st und ts gleiche Ordnung.

Auch für beliebige abstrakte Operatoren a und b gilt der Satz, daß ab und ba gleiche Ordnung haben, falls diese Ordnungen endlich sind. Denn es ist für jedes ϱ als Exponent

$$(ab)^{\varrho+1} = a(ba)^{\varrho}\,b\,;$$

nehmen wir für ϱ die Ordnung von ab, so entsteht hieraus

$$ab = a(ba)^{\varrho}\,b\,, \quad 1 = (ba)^{\varrho}\,,$$

d. h. die Ordnung von ba ist ein Teiler der Ordnung von ab; nimmt man für ϱ die Ordnung von ba, so entsteht

$$(ab)^{\varrho+1} = ab\,, \quad (ab)^{\varrho} = 1\,,$$

d. h. die Ordnung von ab ist ein Teiler der Ordnung von ba. Folglich haben ab und ba gleiche Ordnungen.

§ 34. Wenn die Transformierte des Operators a durch b, also $b^{-1}ab$ mit a übereinstimmt, so heißen a und b miteinander vertauschbar; denn aus

(3) $$b^{-1}ab = a \quad \text{folgt} \quad ab = ba\,.$$

Sind zwei Operatoren a, b miteinander vertauschbar, so ist jede Potenz des einen mit jeder Potenz des anderen vertauschbar. Denn man hat die Gleichungsreihe

$$ba^2 = ba \cdot a = ab \cdot a = a \cdot ba = a \cdot ab = a^2 b\,,$$
$$\cdots\cdots\cdots\cdots$$
$$ba^\mu = a^\mu b\,,$$
$$b^2 a^\mu = b \cdot ba^\mu = ba^\mu \cdot b = a^\mu b^2\,,$$
$$\cdots\cdots\cdots$$

und so allgemein

(4) $$b^\nu a^\mu = a^\mu b^\nu\,.$$

Das zeigt weiter: Jedes Kompositionsresultat zweier vertauschbaren Operatoren a, b läßt sich auf jede der beiden Formen $a^\alpha b^\beta$ oder $b^\beta a^\alpha$ bringen. Es wird nämlich nach (4)

$$a^\varkappa b^\lambda a^\mu b^\nu \ldots = a^{\varkappa+\mu+\cdots} \cdot b^{\lambda+\nu+\cdots} = b^{\lambda+\nu+\cdots} \cdot a^{\varkappa+\mu+\cdots}\,.$$

Folglich hat in der Gruppe, die aus den beiden vertauschbaren Operatoren a und b entsteht,

$$G = \{a, b\}$$

jeder Operator die angegebene Form. Ist also α die Ordnung von a und β die von b, dann kann jeder Operator von G durch ein Produkt

$$a^\mu b^\nu \quad (\mu = 0, 1, 2, \ldots, \alpha - 1;\ \ \nu = 0, 1, 2, \ldots, \beta - 1)$$

dargestellt werden. Es fragt sich aber noch, ob dies nur auf eine Art möglich ist, oder ob auch mit anderen Exponenten σ, τ

$$a^\mu b^\nu = a^\sigma b^\tau \qquad (\mu, \sigma < \alpha;\ \ \nu, \tau < \beta)$$

sein kann. Aus dieser Gleichung würde folgen

$$a^{\mu-\sigma} = b^{\tau-\nu}\,,$$

d. h. es müßte eine Potenz von b mit einer Potenz von a

übereinstimmen. Dabei würde aus der Annahme $\mu = \sigma$ folgen $\tau = \nu$, so daß dieser Fall ausgeschlossen werden kann. Es sei nun b^σ die niedrigste Potenz von b, die gleich einer Potenz von a wird; das sei angedeutet durch

$$b^\sigma = a^\varrho \qquad (\sigma \min) .$$

Dann werden alle Potenzen von b^σ dieselbe Eigenschaft haben, wie das ja klar ist. Und auch nur sie; denn aus einer Gleichung von der Form

$$b^{\varkappa\sigma+\varkappa_1} = a^\gamma \qquad (0 < \varkappa_1 < \sigma)$$

folgt

$$b^{\varkappa_1} = b^{\varkappa\sigma+\varkappa_1} \cdot b^{-\varkappa\sigma} = a^\gamma a^{-\varkappa\varrho} = a^{\gamma-\varkappa\varrho} ,$$

so daß gegen die Voraussetzung schon die $\varkappa_1$te Potenz von b gleich einer Potenz von a wird, obwohl $\varkappa_1 < \sigma$ ist.

Da $b^\beta = 1 = a^\alpha$ ist, also b^β zu $\{a\}$ und folglich zu den Potenzen von b^σ gehört, so wird β ein Vielfaches von σ. Wir setzen nun

$$\beta = \sigma \cdot v ,$$

so daß v eine ganze Zahl bedeutet. Dann kann jede Potenz von b auf die Form $a^\mu b^\nu$ gebracht werden, wobei ν einen der Werte $0, 1, 2, \ldots, (\sigma - 1)$ hat; und jeder Operator von G kann auf die Form gebracht werden

$$a^\mu b^\nu \quad (\mu = 0, 1, 2, \ldots, \alpha - 1;\ \nu = 0, 1, 2, \ldots, \sigma - 1) .$$

Diese Darstellung ist jetzt nur auf eine einzige Art möglich. Demnach ist die Ordnung von G gleich

$$(5) \qquad \alpha \cdot \sigma = \frac{\alpha \cdot \beta}{v} .$$

In derselben Art kann man für die Darstellung der Operatoren von G die Form

$$b^\nu a^\mu \quad (\nu = 0, 1, 2, \ldots, \beta - 1;\ \mu = 0, 1, 2, \ldots, \alpha - 1)$$

wählen. Ist a^τ die niedrigste Potenz von a, die gleich einer Potenz von b wird, so folgt wie oben, daß τ ein Teiler von α ist, so daß man hier

$$\alpha = \tau \cdot \omega$$

bei ganzzahligem ω einsetzen kann. Dann geben die $\beta \cdot \tau$ Operatoren der Form

$$b^\nu a^\mu \quad (\nu = 0, 1, 2, \ldots, \beta - 1;\ \mu = 0, 1, 2, \ldots, \tau - 1)$$

alle Operatoren von G und jeden nur einmal. Also wird die Ordnung von G

(6) $$\beta \cdot \tau = \frac{\alpha \cdot \beta}{\omega},$$

und man findet durch Vergleichung von (5) mit (6) $v = \omega$, also

$$\alpha = \tau \cdot v, \ \beta = \sigma \cdot v; \quad \alpha \sigma = \beta \tau .$$

Ist bei den vertauschbaren Operatoren a und b die Potenz b^σ die niedrigste von b, die einer Potenz von a, und a^τ die niedrigste, die einer Potenz von b gleich wird, hat ferner a die Ordnung α und b die Ordnung β, so ist

(7) $$\alpha \sigma = \beta \tau ,$$

und die Ordnung von $G = \{a, b\}$ ist $\alpha \sigma = \beta \tau$. Für teilerfremde α, β ist die Ordnung von G gleich $\alpha \cdot \beta$.

§ 35. Gruppen, deren Operatoren sämtlich untereinander vertauschbar sind, heißen vertauschbare Gruppen oder Abelsche Gruppen. Dafür, daß eine Gruppe G eine Abelsche sei, reicht es aus, daß alle konstituierenden Elemente $a, b, c, \ldots$ von $G = \{a, b, c, \ldots\}$ untereinander zu je zweien vertauschbar sind.

Jede aus einem Operator gebildete Gruppe $G = \{a\}$ ist eine Abelsche.

Sind alle Operatoren einer Gruppe von der Ordnung 2, so ist die Gruppe eine vertauschbare. Denn bedeuten a und b zwei Operatoren der Gruppe, und ist der Voraussetzung gemäß

$$a^2 = 1, \quad b^2 = 1, \quad (a b)^2 = 1,$$

so folgt zunächst hieraus

$$a = a^{-1}, \quad b = b^{-1}, \quad a b = (a b)^{-1} = b^{-1} a^{-1}$$

und aus diesen drei Resultaten weiter

$$a b = b^{-1} a^{-1} = b a,$$

d. h. a und b sind untereinander vertauschbar.

Wir werden uns weiterhin noch eingehend mit solchen Abelschen Gruppen zu beschäftigen haben.

§ 36. Im § 31, S. 47 haben wir gesehen, daß die Transformation aller Operatoren einer Gruppe G durch

einen unter ihnen wieder auf die Gruppe G zurückführt. Das gleiche kann auch dann eintreten, wenn die Transformierende nicht zu G gehört. Beispielsweise ist der Teiler $G = [1, a, a^2]$ der Gruppe (5) aus § 17, S. 27 von der Eigenschaft, daß $b^{-1} G b = G$ wird; ebenso gilt für die Substitutionengruppe $G = [1, (123), (132)]$ der drei Elemente 1, 2, 3 die Beziehung

$$(12)^{-1} G (12) = (13)^{-1} G (13) = (23)^{-1} G (23) = G ;$$

und es bleibt auch die Transformierte der alternierenden Substitutionengruppe bei Verwendung einer beliebigen Substitution zweiter Klasse (S. 12) ihrer Elemente ungeändert.

Tritt dieser Umstand bei der Transformation der Gruppe G durch den fremden Operator a auf, so wird die Gleichung befriedigt

$$(8) \qquad a^{-1} G a = G \quad \text{oder} \quad a G = G a ,$$

die da aussagt: die Transformierte jedes Operators von G durch a ist wieder ein Operator von G. Wir nennen dann den Operator a mit der Gruppe G vertauschbar. Ist also $G = [b_1, b_2, b_3, \ldots, b_r]$, dann muß für jedes $\varkappa$ ein λ bestehen, für das

$$(9) \qquad a^{-1} b_\varkappa a = b_\lambda \quad \text{oder} \quad b_\varkappa a = a b_\lambda$$

wird. Die Gleichungsreihe (9) ist also mit (8) gleichbedeutend.

Ist G mit a vertauschbar, so auch mit jeder Potenz von a. Denn man hat

$$a^{-2} G a^2 = a^{-1} (a^{-1} G a) a = a^{-1} G a = G ; \ldots$$

Ist G mit a und mit b vertauschbar, so auch mit $a \cdot b$. Denn man hat

$$(a b)^{-1} G a b = b^{-1} (a^{-1} G a) b = b^{-1} G b = G .$$

Ist G mit $a, b, c, \ldots$ einzeln vertauschbar, so auch mit $a^\alpha b^\beta c^\gamma \ldots$

Ist eine Gruppe $G = [b_1, b_2, b_3, \ldots, b_r]$ mit dem Operator a vertauschbar, dann kann jeder Operator von $H = \{G, a\}$ jede der beiden Formen

$$a^\varkappa b_\lambda \quad \text{oder} \quad b_\lambda a^\varkappa$$

$$(\lambda = 1, 2, \ldots, r-1, r; \quad \varkappa = 0, 1, 2, \ldots, \alpha - 1)$$

annehmen, wobei α die Ordnung von a bezeichnet. Das folgt aus (9). Es fragt sich nun, ob derselbe Operator von H in verschiedener Art auf eine solche Form gebracht werden kann, d. h. ob man setzen kann

$$a^{\varkappa} b_{\lambda} = a^{\mu} b_{\nu} \qquad (\varkappa \neq \mu) .$$

Daraus würde folgen

$$a^{\varkappa - \mu} = b_{\nu} b_{\lambda}^{-1} = b_{\pi} ,$$

so daß eine (von der Einheit verschiedene) Potenz von a zu G gehören würde. Ist a^{τ} die niedrigste Potenz von a, die zugleich ein Operator von G ist, dann kann jeder Operator von H auf die Form

$$a^{\varkappa} b_{\lambda} \quad \text{oder} \quad b_{\lambda} a^{\varkappa}$$

$$(\lambda = 1, 2, \ldots, r-1, r; \;\; \varkappa = 0, 1, 2, \ldots, \tau - 1)$$

gebracht werden, und zwar nur auf eine Art. Folglich hat H die Ordnung $r \cdot \tau$.

Auch hier läßt sich, ähnlich wie in dem besonderen Falle von § 31, S. 48 die Substitutionengruppe G einstufig isomorph auf sich beziehen, indem jedes b_{α} dem $a^{-1} b_{\alpha} a$ zugeordnet wird. Diese isomorphe Beziehung geht in eine Identität über, d. h. jeder Operator ist nur dann sich selbst zugeordnet, wenn a nicht nur mit der Gruppe G, sondern sogar mit jedem einzelnen Operator von G vertauschbar ist.

§ 37. G sei eine abstrakte Gruppe und J ein echter Teiler von G. Dann bildet der Komplex der Operatoren von G, die mit J vertauschbar sind, eine Gruppe H, die ein Teiler von G und ein Vielfaches von J ist. Wir wollen sie Zwischengruppe von J in G nennen. Die Ordnungen von G, H, J seien r, s, t, und es sei $r = s \cdot \sigma$; $s = t \cdot \tau$. Transformieren wir nun die Gruppe J durch einen Operator g aus G, der nicht in der Zwischengruppe H enthalten ist, so ist diese Transformierte J_2 von J verschieden, d. h. J und J_2 stimmen nicht in allen Operatoren überein. Es ist daher

$$g^{-1} J g = J_2 \neq J .$$

Die s Operatoren aus Hg, die wir mit $h_{\varkappa} g$ bezeichnen, transformieren J in das gleiche J_2; denn man hat

$$(Hg)^{-1} J (Hg) = g^{-1} (h_{\varkappa}^{-1} J h_{\varkappa}) g = g^{-1} J g = J_2$$

$$(\varkappa = 1, 2, \ldots, s) .$$

Umgekehrt gilt der Satz, daß nur die Operatoren $h_\varkappa g$ des Komplexes $H g$ die Gruppe J in die Gruppe J_2 transformieren. Denn aus der Annahme

$$k^{-1} J k = J_2 ,$$

daß k das J in J_2 transformiert, folgt ja

$$(k g^{-1})^{-1} J (k g^{-1}) = g J_2 g^{-1} = J ,$$

so daß $k g^{-1}$ zu H gehört. Es kann also gesetzt werden

$$k g^{-1} = h_\varkappa , \quad k = h_\varkappa g .$$

Daraus folgt, daß durch die $s \cdot \sigma$ Operatoren von G der Teiler J in σ voneinander verschiedene Gruppen

(9) $$J, J_2, J_3, \ldots, J_\sigma$$

transformiert wird. Ihre Anzahl σ ist ein Teiler der Ordnung von G. Jedes J_α ist selbst wieder eine Untergruppe von G. Die Zwischengruppe H kann in extremen Fällen mit J oder auch mit G übereinstimmen. Ist das letzte der Fall, ist also J mit jedem Operator von G vertauschbar, dann nennen wir G zusammengesetzt und J einen selbstkonjugierten Teiler von G. Ist kein solcher in G vorhanden, so heißt G einfach. Auf diese Verhältnisse werden wir noch näher einzugehen haben.

§ 38. Genau die ähnlichen Überlegungen kann man anstellen, wenn man statt des Teilers J einen Operator i aus G betrachtet. Auch hier gibt es eine Zwischengruppe H, die aus allen in G enthaltenen und mit i vertauschbaren Operatoren besteht. Alle Operatoren $H g_\lambda$ transformieren bei demselben λ den Operator i in denselben Operator i_λ, und nur sie tun das. Auch hier sei $r = s \cdot \sigma$ die Ordnung von G, ferner $s = t \cdot \tau$ die von H, und t die Ordnung von i oder von $\{i\}$. Dann kann i durch Transformation mit den $s \cdot \sigma$ Operatoren von G in σ voneinander verschiedene Operatoren

(9′) $$i, i_2, i_3, \ldots, i_\sigma$$

umgeformt werden, wo σ ein Teiler von r ist.

Die Gesamtheit von (9) oder (9′) heißt ein Transformationskomplex, σ seine Ordnung. Die Operatoren von (9) oder (9′) heißen konjugiert zueinander.

Ein solcher Transformationskomplex ist durch jedes

seiner Elemente vollständig bestimmt; denn ist J_α oder i_α eine Transformierte von J bzw. von i, dann auch J oder i von J_α bzw. von i_α. Bei $\sigma = 1$ heißt i ein selbstkonjugierter Operator von G; ein solcher ist demnach mit allen Operatoren g_λ der zugrunde gelegten Gruppe G vertauschbar, $g_\lambda^{-1} i g_\lambda = i$; $i g_\lambda = g_\lambda i$.

§ 39. Man kann alle Operatoren einer Gruppe G in einer Anzahl von Transformationskomplexen einordnen, derart, daß jeder Operator einmal und nur einmal in einem solchen Komplexe auftritt. Folglich ist die Summe der Ordnungen aller hierbei aufzustellenden Komplexe gleich der Ordnung der Gruppe G, die wieder mit r bezeichnet werde. Eine der Ordnungszahlen zum mindesten hat den Wert 1; denn der Einheitsoperator ist sich selbst konjugiert, bildet also für sich einen Transformationskomplex. Man hat daher

$$(10) \qquad r = 1 + \sigma_2 + \sigma_3 + \dots + \sigma_k ;$$

jedes der σ_α wird ein Teiler von r, der gleich dem Index der Zwischengruppe des zugehörigen Operators ist.

Hiervon wollen wir sofort eine Anwendung machen, indem wir r gleich einer Primzahlpotenz p^α setzen. Da alle σ Teiler von p^α und Vielfache von p sind, wenn sie nicht $=1$ werden, so folgt, daß mindestens noch $(p-1)$ der Ordnungszahlen σ den Wert 1 haben. Mit anderen Worten: Jede Gruppe, deren Ordnung eine Primzahlpotenz p^α ist, hat außer der Einheit mindestens noch $(p-1)$ selbstkonjugierte Operatoren. Die sämtlichen selbstkonjugierten Operatoren einer Gruppe bilden nun eine Untergruppe, da das Produkt zweier auch wieder selbstkonjugiert ist. Man hat folglich: Jede Gruppe, deren Ordnung eine Primzahlpotenz p^α ist ($\alpha > 1$), ist zusammengesetzt (§ 37).

§ 40. Zwei Gruppen

$$G = [a_1, a_2, \dots, a_r] \quad \text{und} \quad H = [b_1, b_2, \dots, b_s]$$

heißen miteinander vertauschbar, wenn die beiden Komplexe von Operatoren

$$(11) \qquad a_\varkappa b_\lambda \quad \text{und} \quad b_\sigma a_\varrho$$

$$(\varkappa, \varrho = 1, 2, \dots, r; \quad \lambda, \sigma = 1, 2, \dots, s)$$

in ihrer Gesamtheit miteinander übereinstimmen, wenn also zu jedem Indexpaare $\varkappa$, λ ein anderes Indexpaar ϱ, σ gefunden werden kann, für das die Gleichung besteht

(11a) $$a_\varkappa b_\lambda = b_\sigma a_\varrho \, .$$

Wir schreiben dies kurz

$$GH = HG \, ,$$

wobei die Elemente a und b, die links aus G und H entnommen sind, mit den rechts entnommenen nicht übereinzustimmen brauchen.

Wir untersuchen die Gruppe, die aus zwei vertauschbaren Gruppen gebildet wird,

$$K = \{G, H\} \, .$$

Die Ordnungen von G und H seien r und s. Die Operatoren von K sind von der Form $a_\varkappa b_\lambda a_\mu b_\nu \dots$ Diese Form reduziert sich durch fortgesetzte Verwendung von (11a) auf die Form $a_\varkappa b_\lambda$ oder ebenso auch auf $b_\lambda a_\varkappa$. Folglich hat K höchstens die Ordnung $r \cdot s$. Es fragt sich, wenn man die Ordnung genau bestimmen will, ob und unter welchen Bedingungen eine Gleichung der Gestalt

(12) $$a_\varkappa b_\lambda = a_\mu b_\nu \qquad (\varkappa \neq \mu \, ; \quad \lambda \neq \nu)$$

bestehen kann. Aus ihr würde folgen $a_\varkappa^{-1} a_\mu = b_\lambda b_\nu^{-1}$, d. h. wir hätten einen Operator, der sowohl G wie H angehört und der dabei von der Einheit verschieden ist. Er gehört zu (§ 22, S. 35)

$$\}G, H\{ = [c_1 , c_2 , c_3 , \dots, c_t] \, ,$$

dem größten gemeinsamen Teiler von G und H. Setzen wir also $a_\varkappa^{-1} a_\mu = b_\lambda b_\nu^{-1} = c_\varrho$, so ergibt sich daraus

(13) $$a_\mu = a_\varkappa c_\varrho \, , \quad b_\nu = c_\varrho^{-1} b_\lambda \qquad (\varrho = 1, 2, 3, \dots t) \, .$$

Und aus diesen Gleichungen folgt umgekehrt (12). Es sind also alle durch (13) bestimmten a_μ, b_ν von der Art, daß sie (12) befriedigen; daher sind je t Operatoren $a_\varkappa b_\lambda$ einander gleich und nur so viele. Sind G und H miteinander vertauschbar, und haben G, H, $\}G, H\{$ die Ordnungen r, s, t, so hat $\{G, H\}$ die Ordnung $\frac{r \cdot s}{t}$.

Wir bemerken noch folgendes über die Arten der Vertauschbarkeit, die bei zwei Gruppen M und N auftreten kann.

Wir setzen

$$M = [m_1, m_2, m_3, \ldots], \quad N = [n_1, n_2, n_3, \ldots].$$

Sind M und N miteinander vertauschbar, d. h. ist jedes Produkt $m_\alpha n_\beta$ auch in der Form $n_\gamma m_\delta$ darstellbar, so schreiben wir

$$M N = N M \quad \text{oder} \quad M N M = M^{-1} N M = N.$$

Ist M dagegen mit allen Operatoren von N vertauschbar, d. h. ist jedes $n_\alpha^{-1} m_\beta n_\alpha$ gleich einem m_γ, also $m_\beta n_\alpha = n_\alpha m_\gamma$, so schreiben wir

$$M \bar{N} = N M \quad \text{oder} \quad \bar{N}^{-1} M \bar{N} = M;$$

der Strich über dem Gruppensymbol N soll andeuten, daß der gleiche Operator der Gruppe N zu nehmen ist.

Ist endlich jeder Operator von M mit jedem von N vertauschbar, d. h. ist jedes $m_\alpha n_\beta$ gleich $n_\beta m_\alpha$, so schreiben wir mit Beibehaltung der gleichen Bedeutung

$$\bar{M} \bar{N} = \bar{N} \bar{M} \quad \text{oder} \quad \bar{N}^{-1} M \bar{N} = \bar{M}.$$

§ 41. Wir heben noch das Theorem hervor: Sind M und N teilerfremde Gruppen, also $\}M, N\{ = 1$, und ist M mit allen Operatoren von N und N mit allen von M vertauschbar, so ist jeder Operator von M mit jedem von N vertauschbar.

In der Tat folgt aus der Voraussetzung

$$\begin{aligned} m_\alpha^{-1} n_\beta^{-1} m_\alpha n_\beta &= (m_\alpha^{-1} n_\beta^{-1} m_\alpha) n_\beta = n_\gamma n_\beta = n_\tau \\ &= m_\alpha^{-1} (n_\beta^{-1} m_\alpha n_\beta) = m_\alpha^{-1} m_\delta = m_\sigma, \end{aligned}$$

so daß der linksstehende Operator sowohl zu M wie zu N gehört, und da M, N teilerfremd sind, nur gleich 1 sein kann. Aus diesem Resultate

$$m_\alpha^{-1} n_\beta^{-1} m_\alpha n_\beta = 1$$

ergibt sich dann $m_\alpha n_\beta = n_\beta m_\alpha$; und damit ist die Richtigkeit des Satzes nachgewiesen.

In diesem Falle ist wegen $\}M, N\{ = 1$ das kleinste gemeinsame Vielfache von M und N

$$(14) \qquad \{M, N\} = [m_\alpha n_\beta] = [n_\beta m_\alpha] ;$$

also wird die Ordnung von $\{M, N\}$ gleich dem Produkte der Ordnungen von M und N. Wir nennen, wenn (14) gilt, die Gruppe $\{M, N\}$ das direkte Produkt der Gruppen M und N; auch bei mehreren Gruppen M, N, P, ... soll die gleiche Bezeichnung gelten.

Diese Bildung direkter Produkte tritt bei Substitutionengruppen stets dann auf, wenn die Gruppen keine gemeinsamen Elemente besitzen; das ist offenbar ein besonderer Fall des eben Besprochenen.

§ 42. Über vertauschbare Gruppen beweisen wir den folgenden Satz: Ist eine Gruppe G mit allen Operatoren einer Gruppe H vertauschbar, so daß also die Gleichungen

$$H^{-1} G \bar{H} = G, \quad \text{d. h.} \quad h_\alpha^{-1} g_\beta h_\alpha = g_\gamma$$

gelten, dann enthält das kleinste gemeinsame Vielfache $\{G, H\}$ der beiden Gruppen G und H die Gruppe G als selbstkonjugierten Teiler.

In der Tat folgt aus der Annahme der Vertauschbarkeit von G und H zunächst, daß jeder Operator von $\{G, H\}$ auf die einfache Form eines Produktes $g_\sigma h_\tau$ gebracht werden kann (§ 40), und daraus ergibt sich weiter

$$\begin{aligned}\overline{\{G, H\}}^{-1} g_\lambda \overline{\{G, H\}} &= (g_\sigma h_\tau)^{-1} g_\lambda (g_\sigma h_\tau) \\ &= h_\tau^{-1} (g_\sigma^{-1} g_\lambda g_\sigma) h_\tau \\ &= h_\tau^{-1} g_\beta h_\tau = g_\gamma ,\end{aligned}$$

d. h. die Transformierte jedes Operators von G gehört wieder zu G. Damit ist der aufgestellte Satz bewiesen.

Ein besonderer Fall hiervon ist der, daß $H = \{h\}$ wird, also G mit h vertauschbar ist. Dann hat man

$$h^{-1} G h = G .$$

Ist $h^{-1} G h = G$, so wird G ein selbstkonjugierter Teiler des kleinsten gemeinsamen Vielfachen $\{G, h\}$ von G und h.

§ 43. G sei eine zusammengesetzte Gruppe der Ordnung r, und J eine Untergruppe der Ordnung t von G, deren Zwischengruppe mit G zusammenfällt; also J ein selbstkonjugierter Teiler von G. Wir haben dann, wenn g_α einen beliebigen Operator von G bedeutet,

$$G^{-1} J G = J \quad \text{oder} \quad g_\alpha^{-1} J g_\alpha = J$$

und

$$g_\alpha J = J g_\alpha .$$

Nun bilden wir die Nebenkomplexe von J in G und zerlegen G in die Summanden

$$\begin{aligned} G &= J + g_2 J + g_3 J + \ldots + g_u J \\ &= J + J g_2 + J g_3 + \ldots + J g_u \qquad (t \cdot u = r) \\ &= J_1 + J_2 + J_3 + \ldots + J_u , \end{aligned}$$

wobei wir $J = J_1$ und $J g_\alpha = g_\alpha J = J_\alpha$ setzen. Gehört das Produkt $g_\alpha g_\beta$ dem Komplex $g_\gamma J$ an, dann ist

$$(g_\alpha J)(g_\beta J) = g_\alpha g_\beta J J = g_\alpha g_\beta J = g_\gamma J ,$$

d. h. das Produkt von J_α und J_β bestimmt sich durch die Gleichung

$$J_\alpha J_\beta = J_\gamma \quad \text{entsprechend} \quad g_\alpha g_\beta = g_\gamma \cdot i_\delta ,$$

wobei i_δ irgend ein der Gruppe J entnommener Operator ist.

Machen wir $J_1, J_2, J_3, \ldots, J_u$ zu Operatoren, deren Komposition durch die soeben abgeleitete Gleichung gegeben wird, so erhalten wir dadurch eine Gruppe Γ der Ordnung u, zu der G in t-stufigem Isomorphismus steht. Dabei entspricht dem Operator J_α in Γ der Komplex der t Operatoren $g_\alpha J$ aus G, und insbesondere der Einheit in Γ die Gruppe $J = J_1$ in G. Wir bezeichnen

$$\Gamma = G/J$$

und nennen Γ die Faktorgruppe von G durch J. Das Symbol G/J hat für uns nur eine Bedeutung, wenn J selbstkonjugiert in G ist.

Ist G zusammengesetzt, so kann sie also als mehrstufig isomorphe zu einer anderen Γ dargestellt werden. Steht umgekehrt G in t-stufigem Isomorphismus zu einer

Gruppe G_1, und entsprechen dem Operator 1 in G_1 die t Operatoren des Teilers J von G, so ist

$$\bar{G}^{-1} J \bar{G} = J ,$$

da dies der Gleichung

$$\bar{G}_1^{-1} \cdot 1 \cdot \bar{G}_1 = 1$$

entspricht. Daher ist J ein selbstkonjugierter Teiler von G, und G ist zusammengesetzt. Eine Gruppe kann dann und nur dann t-stufig isomorph zu einer anderen sein, wenn sie einen selbstkonjugierten Teiler der Ordnung t besitzt.

§ 44. Die Einführung der Faktorgruppe $\Gamma = G/J$ vereinfacht häufig die Untersuchung der Eigenschaften einer Gruppe G, indem diese sich zum Teil in solche zerlegen, die Γ, und in solche, die J besitzt. Durch G und J ist $\Gamma = G/J$ eindeutig bestimmt; dagegen liefern im allgemeinen Γ und J die Gruppe G nicht eindeutig. Es sei z. B., in Substitutionen geschrieben,

$$\Gamma = [1, (\alpha\, \beta)] ; \quad J = [1, (a\, b\, c), (a\, c\, b)] ,$$

so kann G eine der beiden Formen

$$G_1 = [1, (a\, b\, c), (a\, c\, b), (a\, b), (b\, c), (c\, a)] ;$$

$$G_2 = [1, (a\, b\, c), (a\, c\, b), (d\, e), (a\, b\, c)\, (d\, e), (a\, c\, b)\, (d\, e)]$$

annehmen, deren Verschiedenheit ja deutlich zutage tritt. Die Gruppe G_2 erläutert ein allgemein gültiges Bildungsgesetz für G, das darin beruht, die Elemente von Γ und die von J verschieden anzunehmen und dann das direkte Produkt beider Gruppen zu bilden.

§ 45. Unter den selbstkonjugierten Teilern einer Gruppe G verdient ein besonderer vorzüglich Aufmerksamkeit. Das ist der, der aus allen selbstkonjugierten Operatoren der Gruppe G gebildet wird. Nennen wir diesen Teiler H, so ist

$$\bar{G}^{-1} \bar{H} \bar{G} = \bar{H} \quad \text{oder} \quad \bar{H} \bar{G} = \bar{G} \bar{H} .$$

Zu den selbstkonjugierten Operatoren gehört stets der Einheitsoperator. In § 39, S. 56 haben wir die Existenz von mindestens $(p-1)$ von der Einheit verschiedenen, selbstkonjugierten Operatoren in jeder Gruppe der Prim-

zahlpotenzordnung p^λ nachgewiesen. So ist in der Substitutionengruppe der Ordnung 8

$$G = [1, (a\,b), (c\,d), (a\,b)(c\,d), (a\,c)(b\,d), (a\,d)(b\,c), \\ (a\,c\,b\,d), (a\,d\,b\,c)]$$

außer der 1 noch $(a\,b)(c\,d)$ von der besprochenen Eigenschaft

$$\bar{G}^{-1} \cdot (a\,b)(c\,d) \cdot \bar{G} = (a\,b)(c\,d) .$$

Bei den in § 35, S. 52 erwähnten Abelschen oder vertauschbaren Gruppen fällt die Gruppe H der selbstkonjugierten Operatoren mit der gesamten Gruppe G selbst zusammen.

Mit solchen Gruppen H beschäftigt sich der folgende, für spätere Zwecke wichtige Satz.

Die Gruppe H der Ordnung s sei ein Teiler von der Gruppe G der Ordnung $r = s \cdot t$; H enthalte nur selbstkonjugierte Operatoren von G; t und s seien teilerfremd. G ist s-stufig isomorph zur Faktorgruppe $\Gamma = G/H$; die Ordnung von Γ ist also t. Dann entspricht jedem Operator aus Γ genau ein Operator gleicher Ordnung aus G; und umgekehrt entspricht jedem Operator aus G, dessen Ordnung ein Teiler von t ist, genau ein Operator gleicher Ordnung aus Γ.

Zerlegt man nämlich G in H und seine Nebenkomplexe als Summanden (§ 24, S. 36), so erhält man die Gleichung

$$G = H + k_2 H + k_3 H + \ldots + k_\alpha H + \ldots + k_t H .$$

Hieraus leiten wir zunächst eine solche Zerlegung von G her

$$G = H + l_2 H + l_3 H + \ldots + l_\alpha H + \ldots + l_t H ,$$

daß die Operatoren $l_2, l_3, \ldots, l_t$ sämtlich zu Ordnungen nur Teiler von t haben. Zu diesem Zwecke ersetzen wir nach § 15, S. 19 jedes der k_α durch ein Produkt $k_\alpha = l_\alpha \omega_\alpha$, in welchem die Ordnung von l_α ein Teiler von t und die von ω_α ein Teiler von s wird. Das ist auf eine einzige Art möglich (l. c.). Nun betrachten wir die Gruppe $\{\omega_\alpha, H\}$; ihre Ordnung wird gefunden, indem man (§ 40) das Produkt der Ordnungen von ω_α und von H durch die Ordnung von $\}\omega_\alpha, H\{$ dividiert; denn da H in G selbstkonjugiert

ist, so wird ω_α mit H vertauschbar. Die Ordnungen von H, ω_α, $\}\omega_\alpha, H\{$ sind zu t teilerfremd. Ist $\}\omega_\alpha, H\{$ nicht $= H$, d. h. kommt ω_α nicht in H vor, dann ist die Ordnung von $\}\omega_\alpha, H\{$ kleiner als die von ω_α, also die von $\{\omega_\alpha, H\}$ größer als die von H, d. h. $> s$ und teilerfremd zu t. Das ist unmöglich, da das Multiplum G von $\{H, \omega_\alpha\}$ die Ordnung $r = s \cdot t$ hat, also die Ordnung von $\{H, \omega_\alpha\}$ ein Teiler von $s \cdot t$ sein muß. Folglich ist ω_α in H enthalten; man hat demnach

$$\omega_\alpha H = H \quad \text{und} \quad k_\alpha H = l_\alpha H .$$

Wie verlangt war, geht daher die erste Form der Zerlegung von G in die angegebene zweite über.

Nun greifen wir aus $\Gamma = G/H$ einen Operator γ_0 heraus; seine Ordnung sei u, d. h.

$$\gamma_0^u = 1 \qquad (u \min) ;$$

dabei ist u ein Teiler von t. Diesem Operator γ_0 entspricht in G ein Komplex $l_0 H$; und da H mit l_0 vertauschbar ist (§ 15), dem $\gamma_0^u = 1$ der Komplex $l_0^u H$; der muß folglich $= H$ sein, daher $l_0^u = 1$; d. h. die Ordnung von l_0 ist ein Teiler von u. Ist diese Ordnung von l_0 gleich v, so folgt aus $l_0^v = 1$ wegen des Isomorphismus $\gamma_0^v = 1$; d. h. die Ordnung von γ_0 ist ein Teiler von v. Also stimmen γ_0 und l_0 in ihren Ordnungen überein. Ferner sieht man leicht, daß alle anderen Operatoren $l_0 h_\alpha$ aus $l_0 H$ höhere Ordnungen haben als l_0; denn l_0 ist mit jedem Operator von H vertauschbar, also die Ordnung jedes $l_0 h_\alpha$ gleich dem Produkte der Ordnungen von l_0 und von h_α, da die ja teilerfremd zueinander sind.

Umgekehrt sei ein Operator von G gegeben, dessen Ordnung ein Teiler von t ist. Aus dem eben Bewiesenen folgt, daß es nur einer der Reihe $1, l_2, l_3, \ldots, l_\alpha, \ldots, l_t$ sein kann. Das ihm isomorph entsprechende γ hat, wie gezeigt wurde, die gleiche Ordnung wie das l. Damit ist der behauptete Satz in vollem Umfange bewiesen.

§ 46. Ist $\Gamma = G/H$ die Faktorgruppe von G in bezug auf einen zu G selbstkonjugierten Teiler H, so ist auch $\Gamma = \tau^{-1} G \tau / \tau^{-1} H \tau$, wo τ einen ganz beliebigen Operator bedeutet. In der Tat, erzeugt man die Faktorgruppe G/H aus der Zerlegung

$$G = H + g_2 H + \ldots + g_u H ,$$

so ergibt sich $\tau^{-1} G \tau / \tau^{-1} H \tau$ aus der entsprechenden Gleichung

$$\tau^{-1} G \tau = \tau^{-1} H \tau + \tau^{-1} g_2 \tau \cdot \tau^{-1} H \tau + \ldots + \tau^{-1} g_u \tau \cdot \tau^{-1} H \tau ;$$

und ist in der ersten

$$g_\alpha g_\beta = g_\gamma ,$$

so ist

$$\tau^{-1} g_\alpha \tau \cdot \tau^{-1} g_\beta \tau = \tau^{-1} g_\gamma \tau$$

in der zweiten; also haben beide die gleiche Konstitution, d. h. sie sind als abstrakte Gruppen identisch.

---

5. Kapitel.

Zusammengesetzte Gruppen.

§ 47. Zusammengesetzte Gruppen haben wir § 37, S. 54 solche Gruppen genannt, die einen von 1 verschiedenen selbstkonjugierten Teiler niederer Ordnung besitzen. Gruppen, die nicht zusammengesetzt sind, heißen einfache Gruppen (l. c.). Wir wollen eine Reihe von Sätzen über zusammengesetzte Gruppen angeben.

I. Ist K_1 ein eigentlicher Teiler der Gruppe G und umfaßt der Transformationskomplex (§ 38)

$$K_1 , K_2 , K_3 , \ldots, K_q$$

alle zu K_1 konjugierten Gruppen in G, so ist ihr größter gemeinsamer Teiler

$$H = \}K_1 , K_2 , K_3 , \ldots, K_q\{$$

selbstkonjugiert in G; und G ist, falls H nicht mit dem Einheitsoperator zusammenfällt, eine zusammengesetzte Gruppe.

II. Sind H und K selbstkonjugierte Teiler von G, so ist auch $\{H, K\}$ selbstkonjugiert in G.

III. Sind H und K selbstkonjugierte Teiler von G, so ist auch $\}H, K\{$ selbstkonjugiert in G.

IV. Sind zwei Gruppen einstufig isomorph, so sind sie gleichzeitig zusammengesetzt oder gleichzeitig einfach.

Die Beweise für diese vier einfachen Sätze dürfen wir übergehen.

§ 48. Ist H ein selbstkonjugierter Teiler von G, derart, daß kein eigentliches Vielfaches von H, außer G selbst, in G selbstkonjugiert ist, so nennen wir H einen selbstkonjugierten Maximalteiler von G.

V. Ist H ein selbstkonjugierter Maximalteiler von G und ist $\Gamma = G/H$ die zugehörige Faktorgruppe, so ist Γ eine einfache Gruppe. Wäre nämlich Γ zusammengesetzt, so gäbe es in Γ einen echten, von 1 verschiedenen Teiler Δ, für den

$$\bar{\Gamma}^{-1} \Delta \bar{\Gamma} = \Delta$$

wird. Der Gruppe Δ entspräche dann in G eine Gruppe D, die H als Teiler hat (§ 30, S. 45) und die die Gleichung

$$\bar{G}^{-1} D \bar{G} = D \qquad (G > D > H)$$

befriedigt. Danach wäre aber H kein selbstkonjugierter Maximalteiler. (Die Bezeichung $G > D$ ist selbstverständlich.)

VI. Ist H ein selbstkonjugierter Teiler von G und ist $\Gamma = G/H$ eine einfache Gruppe, so ist H ein selbstkonjugierter Maximalteiler von G. In der Tat, wäre dies nicht so, dann gäbe es einen Teiler D von G, der H enthielte und selbstkonjugiert in G wäre. Dem D entspräche ein von 1 und Γ verschiedener selbstkonjugierter Teiler Δ von Γ, und Γ wäre somit nicht einfach.

VII. Sind zwei Gruppen einstufig isomorph, so entspricht jedem selbstkonjugierten Maximalteiler der einen von beiden ein ebensolcher der anderen Gruppe.

Der Beweis hierfür ist ersichtlich.

§ 49. Ist H ein selbstkonjugierter Teiler von G, und sind K und K' zwei andere selbstkonjugierte Teiler von G, die in H enthalten sind, derart, daß H keinen echten Teiler besitzt, der ein echtes Vielfaches von K und auch selbstkonjugiert in G wäre; und ebensowenig einen echten Teiler, der ein echtes Vielfaches von K' und selbstkonjugiert

in G wäre; und ist endlich $L = \}K, K'\{$, so sind die Faktorgruppen

$$H|K, \quad K'|L \quad \text{und ebenso} \quad H|K', \quad K|L$$

einstufig isomorph zueinander.

Aus II, § 47, folgt, daß $\{K, K'\}$ selbstkonjugiert in G ist; ferner ist $\{K, K'\}$ in H enthalten und umfaßt K; also liefert die Voraussetzung als erstes Resultat $\{K, K'\} = H$. Da ferner K und K' selbstkonjugiert in G sind, so sind sie miteinander vertauschbar; man kann also § 40, S. 57 in Anwendung bringen. Bezeichnen wir dazu mit s, s'; t, u die Ordnungen von bzw. K, K'; H, L, so gelten die Gleichungen

(1) $$t = \frac{s\,s'}{u}; \quad \frac{t}{s} = \frac{s'}{u}; \quad \frac{t}{s'} = \frac{s}{u}.$$

Wir setzen $s : u = v$ und geben weiter für die drei Gruppen K, K', L die Bezeichnung ihrer Operatoren durch

$$K = [k_1, k_2, \ldots, k_s], \quad K' = [k'_1, k'_2, \ldots, k'_{s'}];$$
$$L = [l_1, l_2, \ldots, l_u].$$

Aus III, § 47, folgt, daß mit K und K' auch $\}K, K'\{ = L$ selbstkonjugiert in G ist. Man hat daher

(2) $$\begin{cases} K\,k'_\alpha = k'_\alpha\,K; & K'k_\alpha = k_\alpha\,K'; \\ L\,k_\alpha = k_\alpha\,L; & L\,k'_\alpha = k'_\alpha\,L. \end{cases}$$

Wir zerlegen nun K in L und seine Nebenkomplexe als Summanden

(3) $$K = L + k_2\,L + k_3\,L + \ldots + k_v\,L.$$

Ebenso wollen wir H in K' und seine Nebenkomplexe zerlegen. Als erster Summand tritt dabei K' auf. Als zweiten Summanden können wir $k_2\,K'$ annehmen. Denn k_2 gehört wegen (3) zu K; gehörte es auch zu K', dann auch zu $L = \}K, K'\{$, was aber gegen die Bildung von (3) verstoßen würde. Als dritten Summanden dürfen wir $k_3\,K'$ annehmen. Denn nach den eben gemachten Schlüssen gehört k_3 nicht zu K', aber ebensowenig zu $k_2\,K'$, weil aus $k_3 = k_2\,k'_\alpha$ folgen würde $k_2^{-1}\,k_3 = k'_\alpha$ und, da die Faktoren der linken Seite zu K gehören, so wäre $k_2^{-1}\,k_3 = l_\beta$, d. h. $k_3 = k_2\,l_\beta$, was wieder gegen die Bildung

von (3) verstieße. — So kann man weitergehen und jedem Summanden $k_\alpha L$ der Zerlegung von K in (3) einen entsprechenden $k_\alpha L'$ der Zerlegung von H zuordnen. Weil K/L und H/K' gleiche Ordnungen haben, $s:u = t:s' = v$, so wird schließlich

(4) $$H = K' + k_2 K' + k_3 K' + \dots + k_v K'.$$

Die Gleichungen (3) und (4) bestimmen die Faktorgruppen K/L und H/K'; und diese sind einstufig isomorph, da man wegen (2) hat

$$k_\alpha L \cdot k_\beta L = k_\alpha k_\beta L\,; \quad k_\alpha K' \cdot k_\beta K' = k_\alpha k_\beta K'.$$

Genau auf dem gleichen Wege wird der Isomorphismus von K'/L und H/K nachgewiesen.

§ 50. Sind K und K' zwei selbstkonjugierte Maximalteiler der Gruppe H, und ist $L = \}K, K'\{$, so sind die Faktorengruppen

$$H/K,\ K'/L \quad \text{und ebenso} \quad H/K',\ K/L$$

einstufig isomorph; L ist ein selbstkonjugierter Maximalteiler von K und von K'.

Der erste Teil des Satzes folgt aus dem Theoreme des vorigen Paragraphen für $G = H$ als besonderer Fall; der letzte Teil ergibt sich aus dem Umstande, daß nach V, § 48, zunächst H/K und H/K' einfach sind, daß dann nach IV auch K/L und K'/L einfache Gruppen werden, und endlich nach VI, daß L selbstkonjugierter Maximalteiler sowohl von K wie von K' wird.

§ 51. Es sei G eine abstrakte zusammengesetzte Gruppe und G_1 einer ihrer selbstkonjugierten Maximalteiler; G_2 sei ein selbstkonjugierter Maximalteiler von G_1, ferner G_3 von G_2 usw. Dann heißt die Reihe der Gruppen, die mit der Einheit endet

(5) $$G,\ G_1,\ G_2,\ G_3,\ \dots,\ G_{\varrho-1},\ G_\varrho = 1$$
$$(G_\alpha \text{ habe die Ordnung } r_\alpha),$$

eine Kompositionsreihe oder eine Zusammensetzungsreihe von G; die Faktorgruppen

(6) $$G/G_1,\ G_1/G_2,\ G_2/G_3,\ \dots,\ G_{\varrho-1}/G_\varrho = G_{\varrho-1}$$

heißen Kompositionsfaktoren und ihre Ordnungen

$$(7)\qquad \frac{r}{r_1} = e_1\,,\quad \frac{r_1}{r_2} = e_2\,,\quad \frac{r_2}{r_3} = e_3\,,\quad \ldots,\quad \frac{r_{\varrho-1}}{r_\varrho} = e_\varrho$$

heißen Zahlfaktoren der Komposition.

Möglicherweise gibt es für G oder für eins der folgenden Glieder aus (5) mehrere selbstkonjugierte Maximalteiler. Dann ist die Kompositionsreihe nicht eindeutig bestimmt, sondern es gibt verschiedene Aufstellungen (5), (6), (7). Wir untersuchen, um die invarianten Eigenschaften der Zusammensetzungsreihen kennen zu lernen, zunächst den Fall, daß G zwei selbstkonjugierte Maximalteiler G_1 und G_1' besitzt. Dadurch kommen wir auf den im vorigen Paragraphen besprochenen Fall; somit ist $L = \}G_1, G_1'\{$ ein selbstkonjugierter Maximalteiler sowohl von G_1 wie von G_1'. Man kann daher zwei Kompositionsreihen für G herstellen, deren erste Glieder durch

$$G,\ G_1,\ L,\ M,\ \ldots;\quad \text{bzw.}\quad G,\ G_1',\ L,\ M,\ \ldots$$

gegeben sind, und die von L ab übereinstimmen. Sie haben die Kompositionsfaktoren

$$G/G_1\,;\ G_1/L\,;\ L/M\,;\ \ldots;\quad \text{bzw.}\quad G/G_1'\,;\ G_1'/L\,;\ L/M\,;\ \ldots$$

Nach dem vorigen Paragraphen stimmen diese beiden Reihen von Gruppen bis auf die Folge der beiden ersten Faktorgruppen überein.

§ 52. Sind nun für G zwei verschiedene Kompositionsreihen vorhanden, etwa

$$(5)\qquad G,\ G_1,\ G_2,\ G_3,\ \ldots,\ G_\varrho = 1\,,$$

$$(5a)\qquad G,\ G_1',\ G_2',\ G_3',\ \ldots,\ G_\sigma' = 1\,,$$

so läßt sich nachweisen, daß ihre Kompositionsfaktoren bis auf die Folge übereinstimmen. Wir nehmen an, daß dieser Satz für alle Gruppen G richtig sei, deren Ordnung $< r$ ist; daraus soll er für Gruppen der Ordnung r bewiesen werden.

Ist zunächst $G_1 = G_1'$, so sehen wir von G ab und lassen (5) und (5a) mit $G_1 = G_1'$ beginnen; dafür ist der Satz der Annahme nach richtig; also auch für (5) und (5a) selber.

Ist dagegen $G_1 \neq G_1'$, so schieben wir zwischen (5) und (5a) zwei Kompositionsreihen ein

(6) $$G,\ G_1,\ \}G_1,\ G_1'\{,\ H,\ J,\ \ldots,$$

(6a) $$G,\ G_1',\ \}G_1,\ G_1'\{,\ H,\ J,\ \ldots,$$

die sich nur in ihren zweiten Gliedern unterscheiden. Ihre Existenz ist im vorigen Paragraphen gezeigt worden. Von ihnen gilt wegen der Resultate des vorigen Paragraphen der Satz von der Gleichheit der Kompositionsfaktoren. Er gilt aber auch von (5) und (6), und ebenso von (5a) und (6a); also allgemein von (5) und (5a), wenn er für kleinere Werte von r gilt. Der kleinstmögliche Wert für r, bei dem verschiedene Kompositionsreihen auftreten können, ist $r = 4$ bei nichtzyklischen, also Vierergruppen. Wir haben dafür

$$G = [1,\ (x_1 x_2)(x_3 x_4),\ (x_1 x_3)(x_2 x_4),\ (x_1 x_4)(x_2 x_3)]$$

und können bei der Bildung der Kompositionsreihe drei verschiedene selbstkonjugierte Maximalteiler auf G folgen lassen, nämlich, wenn wir

$$g_1 = (x_1 x_2)(x_3 x_4)\ ; \quad g_1' = (x_1 x_3)(x_2 x_4)\ ; \quad g_1'' = (x_1 x_4)(x_2 x_3)$$

setzen, die drei Gruppen zweiter Ordnung

$$G_1 = [1,\ g_1]\ , \quad G_1' = [1,\ g_1']\ , \quad G_1'' = [1,\ g_1'']\ .$$

So haben wir die drei Kompositionsreihen für G

$$G,\ G_1,\ 1\ ; \quad G,\ G_1',\ 1\ ; \quad G_1,\ G_1'',\ 1\ ,$$

und von ihnen gilt das Theorem. Damit ist bewiesen:

Besitzt eine Gruppe mehrere Kompositionsreihen, so stimmen diese in ihren Kompositionsfaktoren, also insbesondere auch in deren Zahlfaktoren überein, abgesehen von der Aufeinanderfolge.

§ 53. Ist M ein selbstkonjugierter Teiler von G, ferner N ein solcher von M usw., so kann man eine Kompositionsreihe von G herstellen, die $M, N, \ldots$ unter ihren Gliedern hat. Ist nämlich M ein selbstkonjugierter Maximalteiler von G, so kann man die Kompositionsreihe sofort mit den beiden Gliedern G, M beginnen. Ist M dagegen kein Maximalteiler von G, so

gibt es einen solchen H unter den Vielfachen von M. Wir beginnen die Kompositionsreihe mit G, H und wenden auf H und M dieselben Überlegungen an. So gelangt man mit M zum Ziele. N wird dann auf gleiche Weise mit M in Beziehung gesetzt, wie dies mit G und mit M geschah; usf.

§ 54. Wir gehen von der Kompositionsreihe

$$G,\ G_1,\ G_2,\ G_3,\ \ldots,\ G_\varrho = 1$$

der Gruppe G aus. Ferner sei H ein beliebiger Teiler von G. Mit ihm bilden wir die Reihe der Gruppen

$$\}G, H\{ = H, \quad \}G_1, H\{ = H_1, \quad \}G_2, H\{ = H_2, \quad \ldots$$
$$\}G_\varrho, H\{ = 1 = H_\varrho .$$

Es ist $H_{\alpha+1}$ für $\alpha = 0, 1, \ldots, \varrho - 1$ in H_α selbstkonjugiert. Um dies zu beweisen, reicht es aus, zu zeigen, daß

$$\overline{H}_\alpha^{-1} G_{\alpha+1} \overline{H}_\alpha = G_{\alpha+1} \quad \text{und} \quad \overline{H}_\alpha^{-1} H \overline{H}_\alpha = H$$

ist. Dann ist auch $\}G_{\alpha+1}, H\{ = H_{\alpha+1}$ mit den Operatoren von H_α vertauschbar. Beides ist ersichtlich. Es folgt aus den beiden Gleichungen

$$\overline{G}_\alpha^{-1} G_{\alpha+1} \overline{G}_\alpha = G_{\alpha+1} \quad \text{und} \quad \overline{H}^{-1} H \overline{H} = H ,$$

sobald man in der ersten dieser beiden Gleichungen für $\overline{G}_\alpha$ den Teiler $\overline{H}_\alpha$ und in der zweiten für $\overline{H}$ den Teiler $\overline{H}_\alpha$ setzt, was offenbar angeht.

Nach dem vorigen Paragraphen kann man also eine Kompositionsreihe von H konstruieren, die unter ihren Gliedern $H_1, H_2, \ldots, H_\varrho$ enthält.

Der Annahme nach enthält G die Gruppe H als Teiler. Nun möge in der Reihe $G, G_1, G_2, \ldots, G_\varrho = 1$ das Glied G_ν das letzte sein, das noch H enthält, so daß man hat

$$\}G_\nu, H\{ = H_\nu = H , \quad \text{aber} \quad \}G_{\nu+1}, H\{ = H_{\nu+1} < H .$$

Da die Natur der Reihe (5), § 51 die Gleichung

$$\overline{G}_\nu^{-1} G_{\nu+1} \overline{G}_\nu = G_{\nu+1}$$

ergibt, so folgt wegen $H < G_\nu$

$$\overline{H}^{-1} G_{\nu+1} \overline{H} = G_{\nu+1} .$$

Hiernach ist $G_{\nu+1}$ mit H vertauschbar, also die Ordnung von $\{G_{\nu+1}, H\}$ gleich dem Produkte der Ordnungen

von $G_{\nu+1}$ und von H, dividiert durch die Ordnung von $\}G_{\nu+1}, H\{ = H_{\nu+1}$. Die Ordnungen von G_ν, $G_{\nu+1}$ seien wie oben, § 51, mit r_ν bzw. $r_{\nu+1}$ bezeichnet, die von H, $H_{\nu+1}$ mit h, $h_{\nu+1}$; dann ist die Ordnung von $\{G_{\nu+1}, H\}$ gleich $\frac{h\, r_{\nu+1}}{h_{\nu+1}}$. Nun ist $\{G_{\nu+1}, H\}$ ein Teiler von $\{G_\nu, H\} = H$. Mithin ist die Ordnung der letzten Gruppe ein Vielfaches der Ordnung der ersten, etwa das $\varkappa$-fache,

$$r_\nu = \frac{h\, r_{\nu+1}}{h_{\nu+1}} \cdot \varkappa ; \qquad \frac{r_\nu}{r_{\nu+1}} = \frac{h}{h_{\nu+1}} \cdot \varkappa .$$

Demnach ist der Zahlenfaktor der Zusammensetzung, der zur Faktorgruppe $H|H_{\nu+1} = H_\nu|H_{\nu+1}$ gehört, ein Teiler des Zahlenfaktors, der zu $G_\nu|G_{\nu+1}$ gehört.

Ebenso wie wir mit H verfuhren, können wir jetzt auch mit $H_{\nu+1}$ verfahren, weil von H nur vorausgesetzt war, es sei ein Teiler von G. Dadurch erkennt man:

Die Zahlfaktoren der Zusammensetzung von G sind Vielfache derjenigen, die zu jedem Teiler H von G gehören.

§ 55. In der Kompositionsreihe von G ist, der Definition gemäß, jedes der Glieder in dem unmittelbar voraufgehenden selbstkonjugiert enthalten. Dabei ist es möglich, daß außer dem zweiten Reihengliede auch noch spätere selbstkonjugiert in G selber sind, wie dies bei dem letzten Gliede, dem Einheitsoperator, ja sicher der Fall ist. Die Glieder der Kompositionsreihe, bei denen dies eintritt, heben wir heraus zu einer neuen Reihe.

Wir bilden also eine Reihe von Gruppen, die mit G beginnt und mit der Einheit endet

(7) $$G,\ H,\ J,\ K,\ \ldots,\ L,\ M,\ N = 1\,,$$

deren Glieder H, J, K, ... Maximalteiler der unmittelbar vorhergehenden Glieder und selbstkonjugiert im Anfangsgliede G sind. Die Bedeutung des Ausdruckes „Maximalteiler" ist klar. Die Reihe (7) nennen wir eine Hauptreihe von G. Aus jeder Hauptreihe läßt sich eine Kompositionsreihe herleiten, indem man nötigenfalls noch Glieder zwischen die der Hauptreihe einschaltet. Das Umgekehrte, daß man durch Unterdrückung einzelner Glieder einer Kompositionsreihe auf eine Hauptreihe gelangt, ist nicht immer

richtig. Beispielsweise hat die Substitutionengruppe des Grades 4 und der Ordnung 8, die wir schon häufiger behandelten,

$$G = [1\,,\ (x_1 x_2)\,,\ (x_3 x_4)\,,\ (x_1 x_2)\,(x_3 x_4)\,,\ (x_1 x_3)\,(x_2 x_4)\,,$$
$$(x_1 x_4)\,(x_2 x_3)\,,\ (x_1 x_3 x_2 x_4)\,,\ (x_1 x_4 x_2 x_3)]$$

die beiden Kompositionsreihen aus je drei Gliedern

$$G_1 = [1\,,\ (x_1 x_3 x_2 x_4)\,,\ (x_1 x_2)\,(x_3 x_4)\,,\ (x_1 x_4 x_2 x_3)]\ ;$$
$$G_2 = [1\,,\ (x_1 x_2)\,(x_3 x_4)]\ ; \quad G_3 = 1$$

und

$$G_1' = [1\,,\ (x_1 x_2)\,,\ (x_3 x_4)\,,\ (x_1 x_2)\,(x_3 x_4)]\ ;$$
$$G_2' = [1\,,\ (x_1 x_2)]\ ; \quad G_3' = 1\,.$$

Dabei ist G, G_1, G_2, G_3 eine Hauptreihe; aus der zweiten G, G_1', G_2', G_3' läßt sich keine Hauptreihe herleiten.

Die aus (7) gebildeten Faktorgruppen aufeinanderfolgender Glieder

$$G/H,\ H/J,\ J/K,\ \ldots,\ L/M,\ M/N = M$$

heißen Kompositionsfaktoren der Hauptreihe, ihre Ordnungen die Zahlfaktoren der Hauptreihe.

§ 56. Besitzt eine Gruppe mehrere Hauptreihen, so stimmen diese in ihren Kompositionsfaktoren, also insbesondere auch in deren Zahlfaktoren derselben überein, abgesehen von der Aufeinanderfolge. Der Beweis dieses Satzes läuft dem des entsprechenden Theorems aus § 51, S. 67 völlig analog; er stützt sich auf das Hilfstheorem aus § 49, S. 65 in der dort bewiesenen allgemeinen Form. Da es sich bei der Darstellung des Beweises nur um eine, zum größten Teile wortgetreue Wiederholung handeln würde, so können wir ihn wohl übergehen.

§ 57. Wir untersuchen nun weiter die Verhältnisse, die da eintreten, wenn zu einer Hauptreihe eine, nicht mit ihr übereinstimmende Kompositionsreihe gehört, wenn also zwischen zwei Glieder der Hauptreihe noch andere Glieder der Kompositionsreihe sich einschieben.

Das geschehe in der Hauptreihe von G

(7) $$G,\ H,\ J,\ K,\ \ldots,\ L,\ M,\ N = 1$$

etwa mit H und J, und zwar möge auf H in der Kompositionsreihe die Gruppe H_1 folgen, die also selbstkonjugierter Maximalteiler von H, aber nicht selbstkonjugiert in G ist. Transformiert man die drei Gruppen H, H_1, J durch alle Operatoren von G, so entstehen die Tripel von Gruppen

(8) $H, H_1, J;\ H, H_2, J;\ H, H_3, J;\ \ldots;\ H, H_q, J,$

wo $H_1, H_2, H_3, \ldots, H_q$ alle zu H_1 konjugierte Gruppen in G sind, also einen Transformationskomplex bilden. Jedes der H_α ist ein echtes Multiplum von J und ein selbstkonjugierter Maximalteiler von H. Infolge dieser Eigenschaften können wir eine Kompositionsreihe von G über H durch jedes der H_α bis J hin aufstellen. Tut man dies mit H_α und H_β, so kann man auf beide Gruppen als Glieder der Kompositionsreihe dieselbe Gruppe

$$H_{\alpha\beta} = \}H_\alpha, H_\beta\{ \qquad (\alpha, \beta = 1, 2, \ldots, q)$$

folgen lassen (§ 52, S. 69). So entstehen die Reihen

(8a) $\ldots, H, H_\alpha, H_{\alpha\beta}, \ldots, J, \ldots$ und $\ldots, H, H_\beta, H_{\alpha\beta}, \ldots, J, \ldots$

Ebenso kann man auch mit H_α und H_γ die Reihe

$$\ldots, H, H_\alpha, H_{\alpha\gamma}, \ldots, J, \ldots$$

bilden. Vergleicht man diese Kompositionsreihe mit der ersten aus (8a), so erkennt man, daß man beide mit dem Gliede

$$H_{\alpha\beta\gamma} = \}H_{\alpha\beta}, H_{\alpha\gamma}\{ = \}H_\alpha, H_\beta, H_\gamma\{$$

fortsetzen kann

(8b) $\ldots, H, H_\alpha, H_{\alpha\beta}, H_{\alpha\beta\gamma}, \ldots, J, \ldots$

In genau derselben Weise können wir als folgendes Glied

$$H_{\alpha\beta\gamma\delta} = \}H_\alpha, H_{\beta\gamma\delta}\{ = \}H_{\alpha\beta}, H_{\gamma\delta}\{ = \ldots$$
$$= \}H_\alpha, H_\beta, H_\gamma, H_\delta\{$$

einführen usf., bis wir auf das Glied

$$H_{1,2,3,\ldots,q} = \}H_1, H_2, H_3, \ldots, H_q\{$$

kommen. Diese Gruppe ist nach I, § 47, S. 64 selbstkonjugiert in G, gehört daher zur Hauptreihe, ist also gleich J.

Nun wird nach § 48, V. S. 65

$$H\,H_1 = H\,H_2 = \ldots = H\,H_q$$

und nach § 50, S. 67

$$H\,H_1 = H_2\,H_{12}\,,$$

also

$$H\,H_1 = H_2\,H_{12} = H_3\,H_{13} = \ldots$$
$$= H_1\,H_{12} = H_3\,H_{23} = \ldots$$

und ebenso weiter. Man findet daher für voneinander verschiedene Indizes α, β, γ, δ, ...

$$H\,H_\alpha = H_\alpha\,H_{\alpha\beta} = H_{\alpha\beta}\,H_{\alpha\beta\gamma} = H_{\alpha\beta\gamma}\,H_{\alpha\beta\gamma\delta} = \ldots$$

Damit ist bewiesen: Stimmt eine Hauptreihe einer Gruppe nicht mit einer zu ihr gehörigen Kompositionsreihe überein, so liefern je zwei aufeinanderfolgende, in der Hauptreihe fehlende Glieder der Kompositionsreihe der Gruppe gleiche Faktorgruppen der Komposition und insbesondere auch gleiche Zahlenfaktoren der Komposition.

§ 58. Wir setzen jetzt der bequemeren Schreibweise halber

$$H_{\alpha\beta\gamma\ldots} = \mathsf{H}_{\delta\varepsilon\zeta\ldots}\,,$$

wo die q Indizes α, β, γ, ..., δ, ε, ζ, ... bis auf ihre Anordnung die sämtlichen Zahlen 1, 2, 3, ..., q darstellen. Dann kann man eine Kompositionsreihe von G über die Glieder

$$\mathsf{H}_{\alpha\beta}\,,\ \mathsf{H}_\alpha\,,\ J \quad \text{oder auch über} \quad \mathsf{H}_{\alpha\beta}\,,\ \mathsf{H}_\beta\,,\ J$$

führen, wie aus dem vorigen Paragraphen ersichtlich ist. H und J sind zwei aufeinanderfolgende Glieder der Hauptreihe, wie dort. Hier sind also H_α sowie H_β selbstkonjugierte Maximalteiler von $\mathsf{H}_{\alpha\beta}$, und J ist ein solcher von H_α sowie von H_β. Aus den Gleichungen

$$\overline{\mathsf{H}}_{\alpha\beta}^{-1}\,\mathsf{H}_\alpha\,\overline{\mathsf{H}}_{\alpha\beta} = \mathsf{H}_\alpha\,, \quad \overline{\mathsf{H}}_{\alpha\beta}^{-1}\,\mathsf{H}_\beta\,\overline{\mathsf{H}}_{\alpha\beta} = \mathsf{H}_\beta$$

folgt dann die Gleichung

$$\overline{\mathsf{H}}_\alpha^{-1}\,\overline{\mathsf{H}}_\beta^{-1}\,\overline{\mathsf{H}}_\alpha\,\overline{\mathsf{H}}_\beta = (\overline{\mathsf{H}}_\alpha^{-1}\,\overline{\mathsf{H}}_\beta^{-1}\,\overline{\mathsf{H}}_\alpha)\,\overline{\mathsf{H}}_\beta = \mathsf{H}_\beta\,\overline{\mathsf{H}}_\beta = \mathsf{H}_\beta$$
$$= \overline{\mathsf{H}}_\alpha^{-1}(\overline{\mathsf{H}}_\beta^{-1}\,\mathsf{H}_\alpha\,\overline{\mathsf{H}}_\beta) = \overline{\mathsf{H}}_\alpha^{-1}\,\mathsf{H}_\alpha = \mathsf{H}_\alpha\,,$$

also, da die linke Seite zu H_α und auch zu H_β gehört und demnach zu $\}H_\alpha, H_\beta\{ = J$, weiter

$$\bar{H}_\alpha^{-1}\,\bar{H}_\beta^{-1}\,\dot{H}_\alpha\,\dot{H}_\beta = J\,,$$

$$\ddot{H}_\alpha\,H_\beta = \bar{H}_\beta\,\bar{H}_\alpha\,J = J\,\bar{H}_\beta\,\bar{H}_\alpha\,,$$

d. h. die Operatoren von H_α sind mit denen von H_β bis auf Operatoren von J vertauschbar.

In dem besonderen Falle, daß J das letzte Glied der Hauptreihe, also $J = 1$ wird, sind die Operatoren jeder Gruppe der Reihe $H_1, H_2, H_3, \ldots, H_q$ mit allen einer jeden anderen Gruppe dieser Reihe vertauschbar. (Dabei brauchen aber die Operatoren der einzelnen Gruppen unter sich selber nicht vertauschbar zu sein.) In dem betrachteten Falle, daß $J = 1$ ist, haben nicht zwei der q Gruppen $H_1, H_2, \ldots, H_q$, die in der Kompositionsreihe der Einheit unmittelbar voraufgehen, einen Operator gemein, da ja

$$\}H_\alpha, H_\beta\{ = J = 1$$

wird. Die Gruppen $\{H_\alpha, H_\beta\}$ haben demnach (§ 41, S. 59) die Eigenschaft, direkte Produkte von H_α und H_β zu sein. Ähnliches gilt für $\{H_\alpha, H_\beta, H_\gamma\} = \{H_{\alpha\beta}, H_\gamma\}$; denn erstens sind die Operatoren von H_γ mit den Operatoren von $H_{\alpha\beta}$ vertauschbar, und zweitens hat $H_{\alpha\beta}$ mit H_γ keinen Operator gemein. Gehören nämlich $\eta_\alpha, \eta_\beta, \eta_\gamma$ bzw. zu H_α, H_β, H_γ, so folgt aus der Annahme $\eta_\gamma = \eta_\alpha \eta_\beta$ sofort $\eta'_\alpha \eta_\gamma = \eta''_\alpha \eta_\beta$, wobei η'_α ein beliebiger Operator aus H_α und $\eta'_\alpha \cdot \eta_\alpha = \eta''_\alpha$ ist. Dann hätten $H_{\alpha\gamma}$ und $H_{\alpha\beta}$ noch Operatoren gemeinsam, die nicht zu H_α gehören. Das widerspricht der Konstitution von $H_\alpha = \}H_{\alpha\beta}, H_{\alpha\gamma}\{$. Geht man so weiter, so zeigt es sich, daß die vorletzte Gruppe H der Hauptreihe das direkte Produkt in G konjugierter Gruppen $H_1, H_2, \ldots, H_q$ wird. Dabei kann $q = 1$ werden; dann ist H eine einfache Gruppe.

Besonders übersichtlich gestalten sich die Verhältnisse, wenn die Ordnung der Gruppe H_1, also auch die der anderen Gruppen $H_2, H_3, \ldots, H_q$ eine Primzahl p wird und somit der letzte Zahlenfaktor der Hauptreihe die $q$te Potenz dieser Primzahl p. Dann ist nämlich H_1 eine zyklische Gruppe, und alle ihre Operatoren sind unter-

einander vertauschbar. Sie sind aber auch, wie wir oben gezeigt haben, mit denen von H_2, H_3, ..., H_q vertauschbar. Demnach ist H eine Abelsche Gruppe der Ordnung p^q, und zwar, wie die vorstehenden Entwicklungen zeigen, vom Typus (1, 1, 1, ..., 1) (vgl. § 69).

§ 59. Als Anwendung der bisherigen Betrachtungen behandeln wir die Gruppen, deren Ordnung die Potenz einer Primzahl p ist. Die betrachtete Gruppe heiße G und die Ordnung von G sei p^α. Am Schlusse von § 39, S. 56 ist gezeigt worden, daß G außer der Einheit noch mindestens $(p-1)$ selbstkonjugierte Operatoren besitzt. Die Ordnung einer jeden von diesen ist (§ 23, S. 36) eine Potenz von p. Es möge p^ϱ die Ordnung des selbstkonjugierten Operators s_0 sein; dann ist die $p^{\varrho-1}$te Potenz von s_0, die wir mit s bezeichnen wollen, ein selbstkonjugierter Operator der Ordnung p, und $\{s\}$ wird eine selbstkonjugierte Untergruppe von G, die die Ordnung p hat. Folglich gibt es eine Faktorgruppe $G/\{s\}$, deren Ordnung durch $p^{\alpha-1}$ gegeben ist, also auch eine Potenz von p wird. Nach dem soeben Bewiesenen hat auch diese Faktorgruppe wieder einen selbstkonjugierten Teiler der Ordnung p. Dem entspricht in G nach § 30, S. 45 eine selbstkonjugierte Untergruppe in G von der Ordnung p^2, die $\{s\}$ enthält; sie möge H heißen. Dann besteht wieder eine Faktorgruppe G/H der Ordnung $p^{\alpha-2}$, aus der weiter die Existenz eines selbstkonjugierten Teilers der Ordnung p^3 in G erschlossen werden kann. So kann man weitergehen und erkennt: Ist die Gruppe G von der Ordnung p^α, so besitzt sie eine Reihe von selbstkonjugierten Teilern zu G

$$(9) \qquad G,\ G_1,\ G_2,\ G_3,\ \ldots,\ G_{\alpha-1},\ 1$$

mit den Ordnungen bzw.

$$p^\alpha,\ p^{\alpha-1},\ p^{\alpha-2},\ p^{\alpha-3},\ \ldots,\ p^1,\ p^0=1\ ,$$

von denen jeder den folgenden enthält. (9) ist demnach eine Hauptreihe von G. — Die Zahlfaktoren jeder Kompositionsreihe einer Gruppe der Ordnung p^α sind sämtlich gleich p. Es fällt aber nicht jede Kompositionsreihe von G mit einer Hauptreihe dieser Gruppe zusammen. Das ist z. B. aus der Gruppe

achter Ordnung ersichtlich, die am Schlusse von § 55, S. 72 behandelt ist.

§ 60. Wir wollen noch bei den Gruppen der Ordnung p^α verweilen und beweisen von ihnen folgenden Satz: Jeder eigentliche Teiler der Ordnung p^ϱ einer Gruppe G der Ordnung p^α ist selbstkonjugiert in einem anderen Teiler von G von der Ordnung $p^{\varrho+1}$.

Es sei H von der Ordnung p^ϱ ein echter Teiler von G, also $0 < \varrho < \alpha$. Hat H mit dem vorletzten Gliede einer Hauptreihe (9), etwa mit $G_{\alpha-1} = \{s\}$ keinen Operator außer der 1 gemein, mit anderen Worten: kommt s nicht in H vor, so kann man den Satz aus § 41, S. 58 anwenden, demzufolge H selbstkonjugiert in $\{H, s\}$ ist, da s mit allen Operatoren von G, also auch mit denen von H vertauschbar ist. Dann besitzt nach § 40, S. 56 $\{H, s\}$ die Ordnung $p^{\varrho+1}$, und H ist ein selbstkonjugierter Teiler in $\{H, s\}$ von der Ordnung $p^{\varrho+1}$ (§ 42, S. 59). In diesem Falle ist daher der Satz als richtig erkannt.

Hat zweitens H mit $G_{\alpha-1} = \{s\}$ außer der Einheit noch einen weiteren Operator s^a gemein, dann ist $\{s\}$ in H enthalten, wie man sofort sieht, da s von der Primzahlordnung p ist. Die Faktorgruppe $G' = G/\{s\}$ enthält einen Teiler H', der dem Teiler H von G entspricht; G' hat die Ordnung $p^{\alpha-1}$ und H' nach § 30, S. 45 die Ordnung $p^{\varrho-1}$.

Auf G' und H' wenden wir die gleichen Schlüsse an wie auf G und H. Dann ist wieder zweierlei möglich: entweder kommt man auf eine Gruppe von der Ordnung p^ϱ, die H' selbstkonjugiert enthält; und dann schließt man auf Grund des Isomorphismus von dieser rückwärts auf einen in G enthaltenen Teiler der Ordnung $p^{\varrho+1}$, der H selbstkonjugiert enthält; — oder man kommt auf zwei neue Gruppen H'' und G'' mit den Ordnungen $p^{\varrho-2}$ und $p^{\alpha-2}$, die zu H bzw. G isomorph sind. Im ersten dieser beiden Fälle ist der Satz bewiesen; im zweiten ist er reduziert. So kann man weitergehen, bis man — im ungünstigsten Falle — zu zwei Gruppen $H^{(\varrho)} = 1$ und $G^{(\varrho)}$ von den Ordnungen 1 und bzw. $p^{\alpha-\varrho}$ gelangt. Für sie ist die Existenz einer Gruppe der Ordnung p klar, die $H^{(\varrho)} = 1$ als selbstkonjugierten Teiler enthält; und somit ist der Beweis des Satzes vollkommen durchgeführt.

Aus diesem Resultate folgt weiter, daß es Kompositionsreihen für G gibt, die einen beliebigen Teiler H von G unter ihren Gliedern haben. Es reicht zur Herstellung einer solchen aus, von H mit der Ordnung p^ϱ auf eine Gruppe K der Ordnung $p^{\varrho+1}$ zurückzugehen, in der H selbstkonjugiert enthalten ist; dann geht man von K in gleicher Weise weiter aufwärts usf., bis man zu G kommt. Dadurch ist die Kompositionsreihe bestimmt.

Ebenso folgt aus dem hergeleiteten Resultate: Jeder Teiler H der Ordnung $p^{\alpha-1}$ der Gruppe G von der Ordnung p^α ist ein in G selbstkonjugierter Teiler.

§ 61. Wir haben gesehen, daß die Gruppe G der Ordnung p^α einen selbstkonjugierten Teiler $\{s\}$ der Ordnung p enthält. Für jeden Operator u von G ist

$$u^{-1} s u = s^\varkappa ;$$

daraus folgt

$$u^{-2} s u^2 = s^{\varkappa^2} ; \quad \ldots ; \quad u^{-r} s u^r = s^{\varkappa^r} .$$

Setzt man $r = p - 1$ und berücksichtigt den Fermatschen Satz, daß

$$\varkappa^{p-1} \equiv 1 \pmod{p}$$

für jedes von Null verschiedene $\varkappa$ ist, so folgt, daß u^{p-1} und s vertauschbar sind. Nun sei u^v die niedrigste Potenz von u, die mit s vertauschbar ist. Dann sind

$$u^v, \; u^{2v}, \; u^{3v}, \; \ldots$$

die einzigen mit s vertauschbaren Potenzen von u. Denn wäre u^t vertauschbar mit s, und läge der Exponent t zwischen $\nu \cdot v$ und $(\nu + 1) \cdot v$, so wäre

$$u^{-(t-\nu v)} s u^{t-\nu v} = u^{-t}(u^{\nu v} s u^{-\nu v}) u^t = u^{-t} s u^t = s ,$$

was gegen die eben gemachte Annahme verstoßen würde. Andrerseits gehören u^{p-1} und u^{p^α} zu den mit s vertauschbaren Potenzen; es müssen also $p - 1$ und p^α den gemeinsamen Teiler v haben. Demnach ist $v = 1$ und $u^{-1} s u = s$, d. h. $\varkappa = 1$.

Also ist nicht nur $\{s\}$ selbstkonjugiert in G, sondern es sind alle einzelnen Operatoren $s, s^2, s^3, \ldots, s^{p-1}$ selbstkonjugierte Operatoren in G.

Das vorletzte Glied $\{s\}$ jeder Hauptreihe von G

besteht aus den Potenzen eines selbstkonjugierten Operators.

§ 62. Die Anzahl aller Teiler H von der Ordnung p^ϱ einer Gruppe G, deren Ordnung gleich p^α ist ($\varrho = 0, 1, 2, \ldots, \alpha$), wird kongruent 1 modulo p. Wir beweisen den Satz auf dem Wege strenger Induktion und nehmen dazu an, er sei für die Ordnungen $p^1, p^2, \ldots, p^{\alpha-1}$ einer Gruppe G bereits als richtig erkannt. Für die Gruppen G der Ordnung p^1 ist dies ja der Fall.

Ist nun eine Gruppe G der Ordnung p^α vorgelegt, so teilen wir sämtliche vorhandenen Teiler der Ordnung p^ϱ von G folgendermaßen in zwei Klassen ein: Wir wählen eine beliebige, aber feste selbstkonjugierte Gruppe $\{s\}$ der Ordnung p von G und rechnen jede Gruppe der Ordnung p^ϱ zur ersten Klasse, wenn sie $\{s\}$ enthält; dagegen zur zweiten Klasse, wenn dies nicht der Fall ist.

Wir behandeln die Teiler der ersten Klasse. Da $\{s\}$ selbstkonjugiert in G ist, können wir die Faktorgruppe $\Gamma = G/\{s\}$ bilden; Γ hat die Ordnung $p^{\alpha-1}$. Jedem ihrer Teiler der Ordnung $p^{\varrho-1}$ entspricht in G ein Teiler der Ordnung p^ϱ, und umgekehrt jedem Teiler der ersten Klasse in G ein Teiler der Ordnung $p^{\varrho-1}$ in Γ (§ 30, S. 45). Für Γ von der Ordnung $p^{\alpha-1}$ ist der aufgestellte Satz als richtig vorausgesetzt. Also sehen wir: Die Anzahl der Teiler von der Ordnung p^ϱ, die zur ersten Klasse gehören, ist kongruent 1 modulo p.

Wir gehen zur Betrachtung der Teiler über, die zur zweiten Klasse gehören. H sei ein solcher Teiler von G, der also $\{s\}$ nicht enthält; seine Ordnung ist p^ϱ. In H gibt es (§ 60) einen für H selbstkonjugierten Teiler J der Ordnung $p^{\varrho-1}$. Wie leicht zu sehen, kann man in H einen Operator u bestimmen, dessen $p$te Potenz die niedrigste der in J vorkommenden ist. Für ihn ist $uJ = Ju$, da J selbstkonjugiert in H ist; ferner hat man

$$H = \{u, J\} = [u^\alpha J] \qquad (\alpha = 0, 1, 2, \ldots, p-1).$$

Nun war s ein Operator aus $\{s\}$, der vorletzten Gruppe der Hauptreihe von G, also nach § 61 selbstkonjugiert in G. In H war s nicht enthalten. Ist jetzt δ ein fester Wert $<p$, so bilden die Operatoren

$$(u s^\delta)^\varkappa \cdot J \qquad (\varkappa = 0, 1, 2, \ldots, p-1)$$

eine Gruppe H_δ. Denn wegen der Vertauschbarkeit von s und u mit J und von s mit u hat man

$$(u\,s^\delta)^\lambda = u^\lambda\, s^{\delta\lambda}\,, \quad J(u\,s^\delta)^\lambda = (u\,s^\delta)^\lambda J\,.$$

Die p Gruppen

$$(10) \qquad H\,,\ H_1\,,\ H_2\,,\ \ldots,\ H_{p-1}$$

sind untereinander verschieden. Denn aus $H_\delta = H_\varepsilon$ würde folgen, daß $u\,s^\delta$ unter den Operatoren von $(u\,s^\varepsilon)^\varkappa J$ vorkäme, also, wenn i_α einen Operator von J bedeutet,

$$u\,s^\delta = u^\varkappa\, s^{\varepsilon\varkappa}\, i_\alpha\,, \quad s^{\delta-\varepsilon\varkappa} = u^{\varkappa-1}\, i_\alpha\,.$$

Die rechte Seite der letzten Gleichung gehört zu H, also ist $\delta \equiv \varepsilon\varkappa \pmod{p}$, und dann, da u nicht zu J gehört, $\varkappa \equiv 1$; $\delta \equiv \varepsilon$.

Es ist daher aus (10) ersichtlich, daß die Teiler H der zweiten Klasse sich in Komplexe von je p Gruppen zusammenstellen lassen: die Anzahl der Teiler zweiter Klasse ist kongruent 0 modulo p. — Die beiden besonderen Resultate geben den allgemeinen Satz.

§ 63. Unabhängig von diesem allgemeinen Beweise zeigen wir die Richtigkeit des Theorems für $\alpha = 2$.

Ist G von der Ordnung p^2 zyklisch, so enthält es je einen Teiler der Ordnung $1, p, p^2$.

Ist G nicht zyklisch, so haben alle von 1 verschiedenen Operatoren die Ordnung p. Es sei s ein selbstkonjugierter Operator von G; ferner sei t ein beliebiger Operator aus G, der nicht in $\{s\}$ vorkommt. Dann ist das folgende Schema geeignet, Einsicht in die Bildung der Teiler der Gruppe G zu geben.

$$\begin{array}{llllll}
1, & t\,, & t^2\,, & t^3\,, & \ldots, & t^{p-1}\,; \\
1, & s\,, & s^2\,, & s^3\,, & \ldots, & s^{p-1}\,; \\
1, & s\,t\,, & (s\,t)^2\,, & (s\,t)^3\,, & \ldots, & (s\,t)^{p-1}\,; \\
1, & s\,t^2\,, & (s\,t^2)^2\,, & (s\,t^2)^3\,, & \ldots, & (s\,t^2)^{p-1}\,; \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
1, & s\,t^{p-1}\,, & (s\,t^{p-1})^2\,, & (s\,t^{p-1})^3\,, & \ldots, & (s\,t^{p-1})^{p-1}\,.
\end{array}$$

Außer der Einheit, die $(p+1)$-mal auftritt, kommen $(p+1)\cdot(p-1) = p^2 - 1$ Operatoren vor. Da s selbst-

konjugiert in G ist, so sind alle diese untereinander verschieden, weil aus

$$(s\,t^{\alpha})^{\beta} = (s\,t^{\gamma})^{\delta} \quad \text{folgen würde} \quad s^{\beta-\delta} = t^{\gamma\delta-\alpha\beta}\,.$$

Die Tabelle umfaßt also alle Operatoren aus G.

Jede Zeile bildet eine zyklische Gruppe, die durch jeden in ihr vorkommenden Operator bestimmt wird. Wir haben also $(p+1)$ solcher zyklischen Gruppen als Teiler von G.

Jede Gruppe, die ein von 1 verschiedenes Glied einer Zeile enthält, umfaßt alle, die zur Zeile gehören.

Gesetzt nun, eine Untergruppe von G enthielte Operatoren aus mehreren Zeilen, die von der Einheit verschieden sind, so wäre die Ordnung dieser Untergruppe $>p$, also $=p^2$, und sie fiele mit G zusammen. Damit ist gezeigt, daß die aufgestellten $(p+1)$ Zeilen der Tabelle alle Teiler der Ordnung p von G erschöpfen.

Der ausgesprochene Satz ist also auch für diesen Typus von Gruppen der Ordnung p^2 richtig. Gleichzeitig sehen wir, daß es für die Ordnung p^2 nur zwei Typen gibt.

§ 64. Wir wollen dieses Kapitel mit einem, der Theorie der Substitutionengruppen angehörigen Satze schließen:

Die alternierenden Substitutionengruppen von mehr als vier Elementen sind einfach.

A sei die alternierende Gruppe von $n(>4)$ Elementen und H eine in ihr selbstkonjugierte Gruppe. Wir betrachten in H die Substitutionen von möglichst geringer Elementenanzahl, die von der Einheitssubstitution verschieden sind; sie müssen regulär sein. Gesetzt, es gäbe ein

$$s_1 = (x_1\,x_2\,x_3\,x_4\,\ldots)\ldots$$

unter diesen Substitutionen, das einen Zyklus von mehr als drei Elementen besitzt. Da $\bar{A}^{-1} H \bar{A} = H$ ist, so kommt in H auch das aus den gleichen Elementen gebildete

$$(x_1\,x_2\,x_3)^{-1}[(x_1\,x_2\,x_3\,x_4\,\ldots)\ldots](x_1\,x_2\,x_3) = (x_2\,x_3\,x_1\,x_4\,\ldots)\ldots$$

vor, und daher auch

$$[(x_1\,x_2\,x_3\,x_4\ldots)\ldots]^{-1}\cdot[(x_2\,x_3\,x_1\,x_4\ldots)\ldots] = (x_3)(x_2\,x_4\ldots)\ldots,$$

d. h. eine nicht identische Substitution, die gegen die Voraussetzung weniger Elemente als s_1 enthält.

Die Substitutionen geringster Elementenzahl haben also nur Zykel von zwei oder von drei Elementen und sind regulär. Sei nun eine von ihnen etwa

$$s_2 = (x_1 x_2)(x_3 x_4) \ldots \quad \text{oder} \quad s_3 = (x_1 x_2 x_3)(x_4 x_5 x_6) \ldots ,$$

so bilden wir die Transformierten durch $\sigma = (x_1 x_2 x_5)$ von s_2 und s_3

$$\begin{aligned} s_2' &= \sigma^{-1} s_2 \sigma & \text{bzw.} \quad s_3' &= \sigma^{-1} s_3 \sigma \\ &= (x_2 x_5)(x_3 x_4) \ldots & &= (x_2 x_5 x_3)(x_4 x_1 x_6) \ldots \end{aligned}$$

H enthält dann auch die von 1 verschiedene Substitution

$$s_2' s_2 = (x_5 x_1 \ldots)(x_3)(x_4) \ldots \quad \text{bzw.} \quad s_3' s_3 = (x_3)(x_1 x_4 \ldots) \ldots$$

mit geringerer Elementenzahl als s_2 bzw. s_3; das widerspricht der Annahme.

Die Substitutionen geringster Elementenzahl haben also eine der Formen

$$(x_1 x_2) \quad \text{oder} \quad (x_1 x_2 x_3) ;$$

die erste ist unmöglich, da A nur gerade Substitutionen besitzt; die zweite liefert für H durch Transformation mit $(x_2 x_\alpha)(x_3 x_\beta)$ alle $(x_1 x_\alpha x_\beta)$ und alle

$$(x_1 x_\alpha x_\beta)(x_1 x_\gamma x_\alpha) = (x_\alpha x_\beta x_\gamma) ,$$

so daß nach § 11, S. 14 H mit A zusammenfällt.

Die Transformation von s_2, s_3 fordert das Vorhandensein von mehr als vier Elementen.

Für $n = 4$ ist die alternierende Gruppe A zusammengesetzt. Ihre Kompositionsreihe ist

$$\begin{aligned} A ; \quad B &= \{(x_1 x_2)(x_3 x_4), (x_1 x_3)(x_2 x_4)\} ; \\ C &= \{(x_1 x_2)(x_3 x_4)\} ; \quad D = 1 . \end{aligned}$$

---

6. Kapitel.

Abelsche Gruppen.

§ 65. Bei unseren früheren Untersuchungen über Operatoren, die miteinander vertauschbar sind, stießen wir bereits in § 35 auf Gruppen, deren Operatoren sämt-

lich die Eigenschaft der Vertauschbarkeit untereinander haben. Wir nannten diese Gruppen Abelsche oder vertauschbare Gruppen. Da für sie neben dem assoziativen auch das kommutative Gesetz gilt, so bilden sie die einfachsten Gruppen und weisen als solche eine Reihe ganz besonderer Eigenschaften auf. Wir wollen diese Gruppen jetzt genauer studieren.

Zunächst führen wir einige, sofort ersichtliche Eigenschaften Abelscher Gruppen an: Jeder Teiler einer Abelschen Gruppe ist wieder eine Abelsche Gruppe. Jeder Teiler ist selbstkonjugierter Teiler der Gruppe. Sind G und H zwei miteinander vertauschbare Abelsche Gruppen (§ 40) der Ordnungen r und s, und hat ihr größter gemeinsamer Teiler $\}G, H\{$ die Ordnung t, so besitzt (§ 42) die Gruppe $\{G, H\}$ die Ordnung $\frac{r \cdot s}{t}$.

§ 66. Es sei F eine Abelsche Gruppe. Jeder ihrer Operatoren, dessen Ordnung keine Primzahlpotenz ist, kann nach § 14 durch zwei oder mehrere vertauschbare Operatoren ersetzt werden, welche Potenzen jenes Operators sind und die selbst Primzahlpotenzen als Ordnungen besitzen. Als solche Primzahlen mögen in F die Zahlen $p, q, r, \ldots$ vorkommen. Wir fassen dann alle Operatoren von F, deren Ordnungen Potenzen von p sind, in einen Komplex zusammen. Sind π_1 und π_2 zwei solche Operatoren, so ist auch $\pi_1 \pi_2$ ein solcher, da wegen der Vertauschbarkeit $(\pi_1 \pi_2)^\alpha = \pi_1^\alpha \pi_2^\alpha$ ist; das Produkt $\pi_1 \pi_2$ gehört demnach auch zu dem Komplexe, d. h. der Komplex bildet eine Gruppe P. Ähnlich bilden die Operatoren, deren Ordnungen Potenzen von q sind, eine Gruppe Q, usw. Es seien $p^\alpha, q^\beta, r^\gamma, \ldots$ die Ordnungen von $P, Q, R, \ldots$

Dann hat man F als direktes Produkt von $P, Q, R, \ldots$, und

$$F = \{P, Q, R, \ldots\} = P \cdot Q \cdot R \cdot \ldots ;$$

denn die rechte Seite ist jedenfalls ein Teiler von F; sie enthält aber auch jeden Operator von F, da ja ein jeder zerlegt worden ist.

Für P und Q sind die Voraussetzungen des letzten Satzes aus dem vorigen Paragraphen erfüllt, und t ist

gleich 1. Somit hat $\{P, Q\}$ die Ordnung $p^\alpha \cdot q^\beta$ und ist $= P \cdot Q$. Ähnlich folgern wir weiter und finden schließlich

$$F = P \cdot Q \cdot R \cdot \ldots ;$$

die Ordnung von F ist $= p^\alpha q^\beta r^\gamma \ldots$

Jede Abelsche Gruppe der Ordnung $p^\alpha q^\beta r^\gamma \ldots$ läßt sich als direktes Produkt Abelscher Gruppen darstellen, deren Ordnungen die Primzahlpotenzen p^α, q^β, r^γ, ... sind. Solchen einfacheren Gruppen wenden wir unsere Aufmerksamkeit zu.

§ 67. G sei eine Abelsche Gruppe, deren Ordnung eine Potenz p^α der Primzahl p ist. Zur Vereinfachung der Schreibweise bezeichnen wir im nächstfolgenden p^α durch $[\alpha]$.

Nun greifen wir willkürlich unter den Operatoren höchster Ordnung von G einen Operator a_1 heraus. Seine Ordnung sei $[n_1]$. Dann bilden wir $\{a_1\}$, d. h. den zyklischen Teiler, der aus den Potenzen von a_1 besteht,

$$(1) \qquad a_1, \; a_1^2, \; a_1^3, \; \ldots, \; a_1^{[n_1]-1}, \; a_1^{[n_1]} = 1 .$$

Die $[n_1]$te Potenz jedes Operators von G ist $= 1$.

Erschöpft (1) alle Operatoren von G, so ist $G = \{a_1\}$ eine zyklische Gruppe.

Erschöpft (1) noch nicht alle Operatoren von G, so durchlaufen wir alle nicht in (1) befindlichen; wir bezeichnen diese durch b. Für ein jedes dieser b gibt es eine niedrigste Potenz, die in (1) vorkommt, da ja sicher die Reihe der Potenzen von b die Einheit enthält, und da 1 zu den Operatoren in (1) gehört; α_2 sei einer der Operatoren aus der Reihe b, für die diese niedrigste Potenz möglichst hoch ausfällt. Der zugehörige Exponent ist ein Teiler der Ordnung von α_2, also eine Potenz von p. Es sei dies die Potenz mit dem Exponenten n_2; dann gehört die $[n_2]$te Potenz jedes Operators von G zum Komplexe (1). Aus der Annahme

$$\alpha_2^{[n_2]} = a_1^\varkappa \quad \text{folgt} \quad \alpha_2^{[n_1]} = 1 = a_1^{\varkappa [n_1 - n_2]}$$

und daraus weiter, daß $\varkappa$ ein Vielfaches von $[n_2]$ ist; denn $\varkappa p^{n_1 - n_2}$ muß ein Vielfaches von p^{n_1} sein. Wir setzen $\varkappa = u[n_2]$, wo u eine ganze Zahl wird, und bilden den Operator

$$a_2 = \alpha_2 \, a_1^{-u} .$$

Der liefert

$$a_2^{[n_2]} = \alpha_2^{[n_2]} a_1^{-u[n_2]} = a_1^{\varkappa} a_1^{-u[n_2]} = 1 ;$$

d. h. a_2 gehört zum Exponenten $[n_2]$; denn die $[n_2]$te Potenz von a_2, nämlich 1, ist die niedrigste in (1) vorkommende. Eine niedere kann offenbar nicht $=1$ sein; denn aus $a_2^{\varrho} = 1 = \alpha_2^{\varrho} a_1^{-u\varrho}$ bei $\varrho < [n_2]$ folgt $\alpha_2^{\varrho} = a_1^{u\varrho}$, so daß schon die ϱte Potenz von α_2 zu (1) gehörte.

Wir betrachten nun den Komplex aller Operatoren, die sich aus a_1 und a_2 bilden lassen,

(2) $$a_1^{\varkappa} a_2^{\lambda}$$

$$(\varkappa = 1, 2, 3, \ldots, [n_1] \quad \text{und} \quad \lambda = 1, 2, 3, \ldots, [n_2]) .$$

Alle diese $[n_1 + n_2]$ Operatoren sind untereinander verschieden, wie leicht zu sehen. Für jeden Operator c aus G folgt $c^{[n_2]} = a_1^{\mu}$ und daraus, wie oben, $\mu = v[n_2]$, wo v eine ganze Zahl wird; dann ist für jeden Operator c aus G

(3) $$c^{[n_2]} = a_1^{v[n_2]} .$$

Erschöpft (2) alle Operatoren von G, dann wird die Gruppe

$$G = \{a_1\} \cdot \{a_2\} = [a_1^{\varkappa} \cdot a_2^{\lambda}]$$

von der Ordnung $[n_1 + n_2]$ werden.

Erschöpft (2) noch nicht alle Operatoren von G, so lassen wir einen Operator alle nicht zu (2) gehörigen Operatoren von G durchlaufen; für jeden von diesen gibt es wegen (3) eine niedrigste Potenz mit einem Exponenten >1 und $\leqq [n_2]$, die in (2) vorkommt. α_3 sei einer von den Operatoren, für welche diese niedrigste Potenz einen möglichst hohen Exponenten, etwa $[n_3]$ hat; dann gehört also die $[n_3]$te Potenz jedes Operators von G zu (2). Aus der Annahme, daß

$$\alpha_3^{[n_3]} = a_1^{\varkappa} a_2^{\lambda}, \quad \text{folgt} \quad \alpha_3^{[n_2]} = a_1^{\varkappa[n_2 - n_3]} a_2^{\lambda[n_2 - n_3]} ;$$

und (3) zeigt dann, daß $\varkappa$ sowie λ Vielfache von $[n_3]$ sind. Wir setzen $\varkappa = u[n_3]$ und $\lambda = v[n_3]$ und bilden den Operator

$$a_3 = \alpha_3 a_1^{-u} a_2^{-v} ;$$

der liefert

$$a_3^{[n_3]} = \alpha_3^{[n_3]} a_1^{-u[n_3]} a_2^{-v[n_3]} = (a_1^{u[n_3]} a_2^{v[n_3]}) a_1^{-u[n_3]} a_2^{-v[n_3]} = 1 .$$

Folglich ist die Ordnung von a_3 ein Teiler von $[n_3]$ und zwar, wie man leicht beweist, der uneigentliche Teiler $[n_3]$ selber. Ist nämlich $\varrho(<[n_3])$ die Ordnung, so wird

$$a_3^\varrho = 1 = \alpha_3^\varrho \, a_1^{-u\varrho} \, a_2^{-v\varrho}\,, \quad \text{also} \quad \alpha_3^\varrho = a_1^{u\varrho} a_2^{v\varrho}\,;$$

dann würde schon die ϱte Potenz von α_1 zu (2) gehören; ϱ kann daher nicht $<[n_3]$ sein.

Alle Operatoren

$$(4) \qquad a_1^\varkappa \, a_2^\lambda \, a_3^\mu$$

$$(\varkappa = 1, 2, \ldots, [n_1]; \quad \lambda = 1, 2, \ldots, [n_2]; \quad \mu = 1, 2, \ldots, [n_1])$$

sind voneinander verschieden. Ihre Zahl ist $[n_1 + n_2 + n_3]$. Für jeden Operator c von G folgt, wie oben, die Gleichung

$$(5) \qquad c^{[n_3]} = a_1^{u[n_3]} \, a_2^{v[n_3]}\,.$$

In dieser Art können wir weitergehen, bis die Operatoren der Gruppe G sämtlich untergebracht sind; und so kommt man auf den Satz: Ist G eine Abelsche Gruppe der Primzahlpotenz-Ordnung p^α, so kann man eine Reihe von Operatoren $a_1, a_2, a_3, \ldots, a_r$ derart auswählen, daß jeder Operator von G auf eine und auch nur auf eine Art in die Form

$$(6) \qquad a_1^{\varkappa_1} \, a_2^{\varkappa_2} \, a_3^{\varkappa_3} \ldots a_r^{\varkappa_r}$$

$$(\varkappa_\varrho = 1, 2, 3, \ldots, [n_\varrho]; \quad \varrho = 1, 2, \ldots, r)$$

gebracht werden kann. Dabei hat jedes a_ϱ die Ordnung $[n_\varrho]$. Die Ordnung von G ist

$$[n_1 + n_2 + n_3 + \ldots + n_r] = p^\alpha\,.$$

Ferner ist

$$(7) \qquad n_1 \geqq n_2 \geqq n_3 \ldots \geqq n_r\,.$$

Für jeden Operator c von G gelten die Gleichungen, in denen die u ganze Zahlen sind,

$$(8) \qquad c^{[n_\varrho]} = a_1^{u_1[n_\varrho]} \, a_2^{u_2[n_\varrho]} \ldots a_{\varrho-1}^{u_{\varrho-1}[n_\varrho]}\,.$$

Die Gesamtheit der Operatoren $a_1, a_2, \ldots, a_r$, die diesen Sätzen entsprechen, nennen wir eine Basis von G.

§ 68. Nach den Darlegungen des vorigen Paragraphen kann eine Basis für eine vorgelegte Abelsche Gruppe G im allgemeinen auf mannigfache Art ausgewählt werden.

Wir wollen nachweisen, daß bei jeder Wahl der Basis die gleichen Zahlen $n_1, n_2, \ldots, n_r$ in gleicher Multiplizität auftreten, so daß auch ihre Anzahl invariant ist. Auf Grund dieses Resultates können wir diese Exponenten n_α nun als Invarianten der Gruppe und insbesondere die Konstante r als den Rang der Gruppe G bezeichnen.

Zum Zwecke des Beweises bestimmen wir die Anzahl N_ϱ der voneinander verschiedenen Operatoren, die in G als $[\varrho]$te Potenzen auftreten. Ist ϱ durch

$$n_{\alpha-1} > \varrho \geqq n_\alpha$$

mit den $n_\varkappa$ verbunden, so wird

$$a_\alpha^{[\varrho]} = 1\,,\ a_{\alpha+1}^{[\varrho]} = 1\,,\ \ldots,\ a_r^{[\varrho]} = 1\,,$$

und die $[\varrho]$te Potenz des allgemeinen Operators (6) in G nimmt die Gestalt an

$$\text{(9)} \qquad a_1^{u_1[\varrho]}\, a_2^{u_2[\varrho]} \ldots a_{\alpha-1}^{u_{\alpha-1}[\varrho]}$$
$$(u_\varkappa = 0\,, 1\,, 2\,, \ldots, [n_\varkappa] - 1)\,.$$

Diese $[n_1 + n_2 + \ldots + n_{\alpha-1}]$ Operatoren (9) sind nicht alle untereinander verschieden; vielmehr wird (9) dann aber auch nur dann gleich einem Operator derselben Form

$$\text{(9a)} \qquad a_1^{v_1[\varrho]}\, a_2^{v_2[\varrho]} \ldots a_{\alpha-1}^{v_{\alpha-1}[\varrho]}$$
$$(v_\varkappa = 0\,, 1\,, 2\,, \ldots, [n_\varkappa] - 1)\,,$$

wenn jedes $v_\varkappa[\varrho] - u_\varkappa[\varrho]$ durch $[n_\varkappa]$, also $v_\varkappa - u_\varkappa$ durch $[n_\varkappa - \varrho]$ teilbar ist. Man erhält daher alle und nur die voneinander verschiedenen $[\varrho]$ten Potenzen, wenn man der Reihe nach jedes $u_\varkappa$ in (9)

$$= 0\,, 1\,, 2\,, \ldots, [n_\varkappa - \varrho] - 1$$

werden läßt. Die gesuchte Anzahl der voneinander verschiedenen $[\varrho]$ten Potenzen ist demnach

$$\text{(10)} \qquad \begin{cases} N_\varrho = [n_1 - \varrho] \cdot [n_2 - \varrho] \ldots [n_{\alpha-1} - \varrho] \\ \qquad = [n_1 + n_2 + \ldots + n_{\alpha-1} - (\alpha - 1)\varrho]\,. \end{cases}$$

Insbesondere wird für $\varrho = n_\alpha$

$$\text{(10a)} \qquad N_{n_\alpha} = [n_1 + n_2 + \ldots + n_\alpha - \alpha\, n_\alpha]\,.$$

Nun sei eine zweite Basis der Gruppe G vorgelegt, etwa

$$b_1\,,\ b_2\,,\ b_3\,,\ \ldots,\ b_s\,.$$

Die zu den b gehörigen Exponenten mögen bzw.

$$[m_1]\,,\ [m_2]\,,\ \ldots,\ [m_s]$$

sein. Aus der Bedeutung von $[m_1]$, die mit der von $[n_1]$ zusammenfällt, erkennt man die Gleichheit der Exponenten $[m_1]$ und $[n_1]$. Wir nehmen nun an, es sei bereits bewiesen, daß auch $m_2 = n_2\,,\ \ldots, m_{\alpha-1} = n_{\alpha-1}$ wird; dann läßt sich zeigen, daß $m_\alpha = n_\alpha$ sein muß.

Gesetzt es wäre $m_\alpha > n_\alpha$, so bilden wir mit Hilfe der $b_\varkappa$ alle $[n_\alpha]$ten Potenzen der Operatoren von G

$$\left(b_1^{\lambda_1[n_\alpha]}\, b_2^{\lambda_2[n_\alpha]} \ldots b_{\alpha-1}^{\lambda_{\alpha-1}[n_\alpha]}\right)\left(b_\alpha^{\lambda_\alpha[n_\alpha]} \ldots b_s^{\lambda_s[n_\alpha]}\right).$$

Um sämtliche in dieser Darstellung enthaltenen verschiedenen Operatoren zu bekommen, lassen wir λ_1 die Reihe $0, 1, 2, \ldots, [m_1 - n_\alpha] - 1$ durchlaufen, denn $b_1^{[n_\alpha]}$ hat die Ordnung $[m_1 - n_\alpha]$. Ferner lassen wir λ_2 die Reihe $0, 1, 2, \ldots, [m_2 - n_\alpha] - 1$ aus ähnlichem Grunde durchlaufen, usf. bis zum letzten Gliede der ersten Klammer des obigen Ausdrucks. Diese Klammer umschließt an verschiedenen Operatoren

$$\begin{aligned}&[m_1 - n_\alpha]\,[m_2 - n_\alpha] \ldots [m_{\alpha-1} - n_\alpha]\\ &= [n_1 - n_\alpha]\,[n_2 - n_\alpha] \ldots [n_{\alpha-1} - n_\alpha]\,;\end{aligned}$$

dies ist nach (10a) gleich N_{n_α}. Also darf die zweite obige Klammer nur den einen Operator 1 liefern; d. h. ihr Wert ist für jede Wahl der $\lambda_\alpha, \ldots, \lambda_s$ gleich 1, daher $[n_\alpha]$ ein Vielfaches von $[m_\alpha]$ und $n_\alpha \geqq m_\alpha$. Das widerspricht aber der obigen Annahme $m_\alpha > n_\alpha$; diese ist also zu verwerfen.

In gleicher Weise läßt sich die Annahme $m_\alpha > n_\alpha$ abtun. Es kommt das ja nur auf eine Veränderung in der Bezeichnung hinaus. Also bleibt allein noch die Möglichkeit $m_\alpha = n_\alpha$ zurück, die demnach eintreten muß. Aus diesem Resultate läßt sich dann auf demselben Wege weiter schließen $m_{\alpha+1} = n_{\alpha+1}\,,\ \ldots,\ m_r = n_r$ und $s = r$. Somit ist bewiesen:

Bei jeder Wahl der Basis einer Abelschen Gruppe mit Primzahlpotenzordnung bleibt die Reihe der Exponenten $n_1, n_2, \ldots, n_r$ und damit auch ihre Anzahl r dieselbe. Diese Zahlen sind also Invarianten der Gruppe.

§ 69. Wir wollen weiter nachweisen, daß diese Invarianten charakteristisch für die Abelschen Gruppen von Primzahlpotenzordnung sind. Dazu zeigen wir: Zwei solche Abelsche Gruppen mit gleichen Invarianten sind einstufig isomorph und daher, als abstrakte Gruppen aufgefaßt, identisch. Infolge der Voraussetzung bestehen die Basen der Gruppen aus gleich vielen Elementen von entsprechend gleicher Ordnung; ihrer absteigenden Größe nach geordnet sind es etwa

$$a_1, a_2, a_3, \ldots, a_r \quad \text{und} \quad b_1, b_2, b_3, \ldots b_r.$$

Wir ordnen jedem a_α als entsprechenden Operator das b_α zu. Dann entsprechen sich auch die Potenzprodukte

$$a_1^{u_1} a_2^{u_2} \ldots a_r^{u_r} \quad \text{und} \quad b_1^{u_1} b_2^{u_2} \ldots b_r^{u_r},$$

und damit ist der einstufige Isomorphismus bewiesen.

Sind umgekehrt zwei Abelsche Gruppen G und H von Primzahlpotenzordnung zueinander einstufig isomorph, so kann man die Operatoren $b_1, b_2, b_3, \ldots, b_r$ von H, die denen der Basis $a_1, a_2, a_3, \ldots, a_r$ von G entsprechen, zu einer Basis der anderen Gruppe H machen; denn die b_α befriedigen auch die den a_α auferlegten Bedingungen. Daraus folgt die Gleichheit der Invarianten und insbesondere des Ranges.

Die Invarianten sind demnach für die Konstitution der Abelschen Gruppen von Primzahlpotenzordnung entscheidend. Den zur Basis (6) gehörigen Typus bezeichnen wir durch $(n_1, n_2, n_3, \ldots, n_r)$. Es gibt für Abelsche Gruppen der Ordnung p^n so viele Typen, als es Zerlegungen von n in gleiche oder ungleiche Summanden gibt, bei denen aber die Permutationen der Summanden nicht als verschiedene Zerlegungen gelten, so daß ihre Anordnung nach abnehmender Größe der Summanden vorgenommen werden darf. Wir geben für $n = 1, 2, 3, 4, 5$ die einzelnen Typen an. Für

p^1 gibt es (1);

p^2 „ „ (2); (1, 1);

p^3 „ „ (3); (2, 1); (1, 1, 1);

p^4 „ „ (4); (3, 1); (2, 2); (2, 1, 1); (1, 1, 1, 1);

p^5 „ „ (5); (4, 1); (3, 2); (3, 1, 1); (2, 2, 1); (2, 1, 1, 1); (1, 1, 1, 1, 1).

Wollen wir die Primzahl p hervorheben oder kenntlich machen, so schreiben wir den Typus ausführlicher $(p^{n_1}, p^{n_2}, \ldots, p^{n_r})$.

Vergleichen wir das eben erhaltene Resultat für p^2 mit dem aus § 63, S. 80, und beachten § 61, S. 78, so folgt, daß jede Gruppe der Ordnung p^2 eine Abelsche Gruppe ist.

§ 70. Liegt nun, wie das zu Anfang des Kapitels angenommen wurde, eine allgemeine Abelsche Gruppe G vor, so kann sie als direktes Produkt

$$G = P \cdot Q \cdot R \ldots$$

dargestellt werden, wo P als Ordnung die höchste Potenz p^m der Primzahl p hat, die in der Ordnung von G enthalten ist, usw. Behandelt man dann $P, Q, R, \ldots$ nach der in den vorigen Paragraphen besprochenen Methode, so möge P die Basiselemente $a_1, a_2, a_3, \ldots$ mit den Ordnungen $p^{m_1}, p^{m_2}, p^{m_3}, \ldots$ $(m_1 \geqq m_2 \geqq m_3 \geqq \ldots)$ besitzen, Q die Basiselemente $b_1, b_2, b_3, \ldots$ mit den Ordnungen $q^{n_1}, q^{n_2}, q^{n_3}, \ldots$ $(n_1 \geqq n_2 \geqq n_3 \geqq \ldots)$, ferner R die $c_1, c_2, c_3, \ldots$ mit $r^{t_1}, r^{t_2}, r^{t_3}, \ldots$ $(t_1 \geqq t_2 \geqq t_3 \geqq \ldots)$ usf. Dann wird

$$G = \{a_1\}\{a_2\} \ldots \{b_1\}\{b_2\} \ldots \{c_1\}\{c_2\} \ldots$$

Die höchste Ordnung, die ein Operator aus G annehmen kann, ist offenbar $p^{m_1} q^{n_1} r^{t_1} \ldots$, und zwar tritt diese Ordnung bei $a_1 \cdot b_1 \cdot c_1 \ldots$ auch wirklich auf. Wir bezeichnen

$$a_1 \cdot b_1 \cdot c_1 \ldots = A_1 .$$

Dann werden $a_1, b_1, c_1, \ldots$ Potenzen von A_1, und wir haben

$$G = \{A_1\} \cdot \{a_2\} \ldots \{b_2\} \ldots \{c_2\} \ldots$$

G ist das direkte Produkt der Faktoren auf der rechten Seite dieser Gleichung.

Wir verfahren nun in entsprechender Weise mit den weiteren Faktoren. Wir setzen

$$a_2 \cdot b_2 \cdot c_2 \ldots = A_2 ;$$

dann hat A_2 die höchste Ordnung, die ein Operator der Gruppe $G/\{A_1\}$ annehmen kann, nämlich $p^{m_2} q^{n_3} r^{t_3} \ldots$; dabei wird

$$\}(\{A_1\} \cdot \{A_2\})\{ = 1 .$$

So gehen wir weiter und können auf die angegebene Art die sämtlichen Operatoren von G erschöpfen. Wir erkennen: Ist G eine beliebige Abelsche Gruppe, so kann man eine Reihe von Operatoren $A_1, A_2, \ldots, A_\varrho$ so auswählen, daß jeder Operator von G auf eine und nur auf eine Art in die Form

$$A_1^{\varkappa_1} A_2^{\varkappa_2} \ldots A_\varrho^{\varkappa_\varrho}$$

gebracht werden kann, wobei $\varkappa_1, \varkappa_2, \ldots, \varkappa_\varrho$ kleiner bleiben als die Ordnungen $\omega_1, \omega_2, \ldots, \omega_\varrho$ der zugehörigen Operatoren $A_1, A_2, \ldots, A_\varrho$. Dabei ist jedes $A_\alpha^{\omega_\alpha}$ die niedrigste Potenz von A_α, die als Potenzprodukt der vorangehenden Elemente

$$A_1^{\lambda_1} A_2^{\lambda_2} \ldots A_{\alpha-1}^{\lambda_{\alpha-1}}$$

darstellbar ist.

§ 71. Wir wollen die studierten Begriffe für die Untersuchung der Gruppen der Ordnung 8 verwenden (vgl. § 17) und die erhaltenen Resultate dann weiter verwerten.

Da die Ordnung einer Gruppe ein Vielfaches der Ordnung jedes Operators ist, so können in einer Gruppe achter Ordnung nur Elemente einer der Ordnungen 1, 2, 4, 8 vorkommen. Kommt ein Operator achter Ordnung vor, so ist die Gruppe zyklisch, also eine Abelsche Gruppe vom Typus (2^3); sind alle Operatoren von der zweiten Ordnung, so ist die Gruppe auch eine Abelsche (§ 35, S. 52) vom Typus $(2^1, 2^1, 2^1)$. Gibt es außer diesen uns bereits bekannten Typen noch andere, so kommt in ihnen sicher

ein Operator a der Ordnung 4 vor. Die Gruppe G besteht demnach in diesem Falle aus den acht Operatoren

$$(11) \qquad 1, a, a^2, a^3; \quad b, ab, a^2b, a^3b,$$

wobei b einen Operator von G bedeutet, der nicht unter den Potenzen von a vorkommt, und b^2 ein Operator von (11) wird.

Nun ist auch ba in (11) enthalten und kann, wie man sofort sieht, nur einer der Operatoren ab, a^2b, a^3b sein. Aus $ba = ab$ würde folgen, daß G eine Abelsche Gruppe ist. Aus $ba = a^2b$ würde folgen

$$ba^2 = ba \cdot a = a^2b \cdot a = a^2 \cdot ba = a^2 \cdot a^2b = a^4b = b,$$

also $a^2 = 1$, was der Annahme über die Ordnung von a widerspricht.

Etwas Neues kann sich daher nur aus der Annahme

$$ba = a^3b$$

ergeben. Das setzen wir demnach voraus.

Weiter muß in (11) auch b^2 vorkommen; man sieht, daß es nur einer der Operatoren $1, a, a^2, a^3$ sein kann. Aus $b^2 = a$ folgt

$$G = \{a, b\} = \{b^2, b\} = \{b\};$$

d. h. G wäre zyklisch. Aus $b^2 = a^3$ schließen wir zuerst $b^6 = a^9 = a$, und dann

$$G = \{a, b\} = \{b^6, b\} = \{b\};$$

also auch hier wäre G zyklisch. Es bleibt daher nur noch $b^2 = 1$ und $b^2 = a^2$ zu untersuchen übrig.

Wir haben somit zwei Möglichkeiten zu betrachten:

$$\text{I.} \quad a^4 = 1, \quad b^2 = 1, \quad ba = a^3b:$$

$$\text{II.} \quad a^4 = 1, \quad b^2 = a^2, \quad ba = a^3b.$$

Diese Festsetzungen reichen für die Aufstellung der Cayleyschen Quadrate aus. Im ersten Falle erhält man

(I)

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

und im zweiten Falle

(II)

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2 .

Setzt man diese Gruppen nach § 18, S. 27 in Substitutionen-Gruppen um, so erhält man, wenn man die Operatoren aus (11) durch die Klammerelemente 1, 2, 3, 4, 5, 6, 7, 8 bezeichnet, im ersten Falle

$$\text{(Ia)}\quad \begin{cases} 1,\ (1234)(5678),\ (13)(24)(57)(68),\ (1432)(5876), \\ (15)(28)(37)(46),\ (16)(25)(38)(47),\ (17)(26)(35)(48), \\ (18)(27)(36)(45) \end{cases}$$

und im zweiten

$$\text{(IIa)}\quad \begin{cases} 1,\ (13)(24)(57)(68),\ (1234)(5678),\ (1432)(5876), \\ (1537)(2846),\ (1638)(2547),\ (1735)(2648), \\ (1836)(2745)\,. \end{cases}$$

Aus diesen Darstellungen folgt sofort, daß (I) und (II) den drei Gruppenbedingungen entsprechen, und ferner, daß

(I) und (II) voneinander wirklich verschieden sind. Das letzte ergibt sich z. B. daraus, daß (I) nur zwei, dagegen (II) sechs Operatoren vierter Ordnung aufweist. Für (II) ist dies unter den Gruppen achter Ordnung eine charakteristische Eigenschaft.

Nach dieser Digression kehren wir zu den Abelschen Gruppen zurück.

§ 72. Wir sahen, daß die Basis einer Abelschen Gruppe auf mancherlei Weise ausgewählt werden kann. Dies führt auf die Frage, auf wieviel verschiedene Arten eine solche Auswahl möglich ist. Wir wollen das nur für den einfachsten Fall einer Gruppe von der Primzahlpotenzordnung p^r mit dem Typus $(1, 1, 1, \ldots, 1)$ von r Einheiten untersuchen. Die Gruppe enthält p^r Operatoren, von denen einer die Ordnung 1 hat, während die $(p^r - 1)$ anderen die Ordnung p haben. Einen der letzten, a_1, wählen wir als erstes Element der Basis; das kann auf $(p^r - 1)$ Arten geschehen; und durch die $(p - 1)$ ersten Potenzen des gewählten Operators werden $(p - 1)$ Operatoren der Ordnung p ausgeschieden. Es bleiben also nur noch $(p^r - p)$ solcher Operatoren zurück. Aus ihnen kann willkürlich ein zweites Element der Basis, a_2, entnommen werden. Dann sind die p^2 Operatoren

$$a_1^s \, a_2^t \qquad (s, t = 1, 2, 3, \ldots, p)$$

voneinander verschieden, und $(p^2 - 1)$ unter ihnen haben die Ordnung p. Es bleiben also von den $(p^r - 1)$ Operatoren der Ordnung p noch $(p^r - p^2)$ übrig, aus denen a_3 auf $(p^r - p^2)$ Arten gewählt werden kann. So geht es weiter; man sieht, daß die r Elemente der Basis auf

$$(p^r - 1)(p^r - p)(p^r - p^2) \ldots (p^r - p^{r-1})$$

Arten gewählt werden können.

§ 73. Die Gruppe (II) des § 71 bietet noch eine bemerkenswerte Erscheinung dar. Es wird nämlich jeder Operator der Gruppe durch jeden anderen der Gruppe in eine seiner Potenzen transformiert. So hat man z. B. in der dortigen Bezeichnung die Relationen

$$a^{-1} b a = b^3 \quad \text{und} \quad b^{-1} a b = a^3 ,$$

und es folgt leicht die ausgesprochene Eigenschaft aus

der Betrachtung und unter Benutzung des zugehörigen Cayleyschen Quadrats. Man findet

$$a^{-1}(a\,b)\,a = (a\,b)^3\,, \quad a^{-1}(a^2 b)\,a = (a^2 b)^3\,, \quad a^{-1}(a^3 b)\,a = (a^3 b)^3\,,$$

$$b^{-1}(a\,b)\,b = (a\,b)^3\,, \quad b^{-1}(a^2 b)\,b = (a^2 b)^3\,, \quad b^{-1}(a^3 b)\,b = (a^3 b)^3\,,$$

. . . .

$$a^{-2}(a\,b)\,a^2 = a\,b\,, \quad a^{-2}(a^2 b)\,a^2 = a^2 b\,, \quad a^{-2}(a^3 b)\,a^2 = a^3 b\,,$$

. . . .

Bei der Gruppe (I) des § 71 besteht diese Eigenschaft nicht. Man hat z. B. bei ihr

$$a^{-1}(a\,b)\,a = b\,a = a^3 b\,,$$

und wegen $(a\,b)^2 = 1$ ist die rechte Seite $a^3 b$ nicht als Potenz von ab ausdrückbar.

Gruppen der angegebenen Eigenschaft stehen den Abelschen besonders nahe; sie können als eine Erweiterung von diesen betrachtet werden. Nach Dedekind heißen sie Hamiltonsche Gruppen. Jede Abelsche Gruppe ist demnach eine Hamiltonsche, aber nicht umgekehrt. Die Gruppe (II) des § 71 ist die einfachste nicht-Abelsche unter den Hamiltonschen Gruppen. Sie führt den Namen Quaternionengruppe. Diese Bezeichnung rechtfertigt sich aus den folgenden Betrachtungen.

In der Theorie der komplexen Zahlen werden vier Einheiten benutzt, ± 1 und $\pm i$, zwischen denen die Beziehung $i^2 = -1$ besteht. In der von W. R. Hamilton begründeten Theorie der Quaternionen treten zu diesen Einheiten noch vier neue $\pm j$ und $\pm k$, und die Verbindung der acht Einheiten untereinander wird durch folgendes Schema festgelegt:

$$i^2 = j^2 = k^2 = -1\,;$$

$$i\,j = k\,, \quad j\,k = i\,, \quad k\,i = j\,;$$

$$j\,i = -k\,, \quad i\,k = -j\,, \quad k\,j = -i\,.$$

Wir erhalten als Multiplikationstabelle, in der das Eingangsglied links den ersten Faktor und das Eingangsglied oben den zweiten Faktor angibt, für diese acht Einheiten durch die eben aufgestellten Beziehungen

(III)

	1	i	-1	$-i$	j	k	$-j$	$-k$
1	1	i	-1	$-i$	j	k	$-j$	$-k$
i	i	-1	$-i$	1	k	$-j$	$-k$	j
-1	-1	$-i$	1	i	$-j$	$-k$	j	k
$-i$	$-i$	1	i	-1	$-k$	j	k	$-j$
j	j	$-k$	$-j$	k	-1	i	1	$-i$
k	k	j	$-k$	$-j$	$-i$	-1	i	1
$-j$	$-j$	k	j	$-k$	1	$-i$	-1	i
$-k$	$-k$	$-j$	k	j	i	1	$-i$	-1

Setzt man hierin

$$i = a\,, \quad j = b\,, \quad k = a\,b\,,$$

so geht (III) in (II) aus § 71 über, d. h. die abstrakte Gruppe (II) ist der Multiplikatorgruppe der acht Quaternioneneinheiten einstufig isomorph.

§ 74. Sind a und b zwei nicht vertauschbare Operatoren einer Hamiltonschen Gruppe, so muß zwischen ihnen eine Gleichung von der Form

$$a^{-1}\,b\,a = b^m \qquad (m > 1) \tag{12}$$

bestehen. Aus ihr folgert man leicht

$$\left\{\begin{aligned} &a^{-\varkappa}\,b^{\lambda}\,a^{\varkappa} = b^{\lambda\cdot m^{\varkappa}}\,,\\ &b^{\lambda}\,a^{\varkappa} = a^{\varkappa}\,b^{\lambda\cdot m^{\varkappa}}\,,\\ &(a\,b)^{\varkappa} = a^{\varkappa}\,b^{1+m+m^2+\ldots+m^{\varkappa-1}}\,. \end{aligned}\right. \tag{13}$$

Aus der letzten Formel kann man schließen, daß, wenn a und b zu Ordnungen p^{α} und p^{β}, also Potenzen derselben Primzahl p haben, daß dann für $a \cdot b$ das gleiche der Fall ist. Denn nehmen wir zuerst $\varkappa = p^{\alpha}$, dann folgt

$$(a\,b)^{p^{\alpha}} = b^{1+m+\cdots}\,,$$

und erheben wir ferner diese Gleichung zur p^{β}ten Potenz, so ergibt sich

$$(a\,b)^{p^{\alpha+\beta}} = 1\,;$$

demnach ist die Ordnung von $(a\,b)$ ein Teiler von $p^{\alpha+\beta}$, d. h. selbst wieder eine Potenz der Primzahl p. Nun beruhte gerade auf diesem Umstande der in § 66, S. 83

gegebene Beweis des Theorems von der Zerfällung Abelscher Gruppen in ein direktes Produkt. Hier können wir genau ebenso vorgehen zur Bestätigung des Theorems: Jede Hamiltonsche Gruppe G der Ordnung $p^\alpha \cdot q^\beta \cdot r^\gamma \cdot \ldots$, wobei $p, q, r, \ldots$ voneinander verschiedene Primzahlen bedeuten, läßt sich als direktes Produkt Hamiltonscher Gruppen $P, Q, R, \ldots$ darstellen, deren Ordnungen die Primzahlpotenzen $p^\alpha, q^\beta, r^\gamma, \ldots$ sind. Es ist also

$$G = P \cdot Q \cdot R \ldots,$$

wo P aus allen Operatoren von G gebildet wird, deren Ordnung eine Potenz von p ist, usw.

§ 75. Bedeuten a und b zwei Operatoren einer Hamiltonschen Gruppe G, so ist

$$a^{-1}ba = b^m, \quad b^{-1}ab = a^n.$$

Hieraus folgt

$$a^{-1}b^{-1}a = (a^{-1}ba)^{-1} = b^{-m},$$

$$(14) \quad \begin{cases} a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) = a^{-1}a^n = a^{n-1} \\ \qquad = (a^{-1}b^{-1}a)b = b^{-m}b = b^{-m+1}, \end{cases}$$

d. h. $a^{-1}b^{-1}ab$ gehört sowohl zu der zyklischen Gruppe $\{a\}$, wie zu der zyklischen Gruppe $\{b\}$. Sind nun a und b verschiedenen Gruppen $P, Q, R, \ldots$ entnommen, so haben $\{a\}$ und $\{b\}$ nur den Einheitsoperator gemeinsam, und es ist

$$a^{-1}b^{-1}ab = 1 \quad \text{oder} \quad ba = ab,$$

d. h. alle Operatoren einer jeden der Gruppen $P, Q, R, \ldots$ sind mit allen Operatoren aller anderen dieser Gruppen vertauschbar. Da durch diese Vertauschbarkeit die Verbindung zwischen den Operatoren der einzelnen Gruppen $P, Q, R, \ldots$ hinsichtlich der Kompositionsvorschriften hergestellt wird, so ist die Konstitution der Gruppe und ihr Cayleysches Quadrat vollkommen bekannt, wenn die der einzelnen Teiler $P, Q, R, \ldots$ von Primzahlpotenzordnung $p^\alpha, q^\beta, r^\gamma, \ldots$ feststeht. Es reicht also aus, Hamiltonsche Gruppen der Ordnung p^α zu untersuchen.

Haben a und b die Ordnungen p^μ bzw. p^ν, so folgt aus (14) sofort wegen $b^{-m+1} = a^{n-1}$, daß die beiden zykli-

schen Gruppen $\{a\}$, $\{b\}$ außer der Einheit noch andere Operatoren gemeinsam haben. Der in (14) eingeführte Operator $a^{-1}b^{-1}ab$ ist von R. Dedekind, der diese Theorie begründete, als Kommutator von a und b bezeichnet worden. Er ist als a^{n-1} mit a und als b^{-m+1} mit b, also mit allen Operatoren von $\{a, b\}$ vertauschbar. Der Kommutator von b und a ist

$$b^{-1}a^{-1}ba = (a^{-1}b^{-1}ab)^{-1}.$$

R. Dedekind hat gezeigt, daß nur für $p = 2$ nichtvertauschbare Hamiltonsche Gruppen einer Primzahlpotenzordnung p^α bestehen. Uns würde das Eingehen auf diese interessanten Untersuchungen zu weit führen.

---

7. Kapitel.

Sätze von Sylow und von Frobenius.

§ 76. Wir haben in § 23, S. 36 bewiesen, daß die Ordnung r einer Gruppe G ein Vielfaches der Ordnung n jedes ihrer Operatoren ist, sowie auch jedes ihrer Teiler. Diese Sätze sind nicht ohne weiteres umkehrbar, d. h. wenn n ein Teiler von r ist, so gibt es in G nicht stets einen Operator oder auch eine Untergruppe von der Ordnung n. Beispielsweise hat die alternierende Substitutionengruppe von vier Elementen (die in § 11, S. 14 angegeben ist), die Ordnung $r = 12$; aber sie enthält weder einen Operator noch eine Untergruppe von der Ordnung $n = 6$. Dagegen ist, wie Cauchy gezeigt hat, die Umkehrung richtig, wenn n gleich einer Primzahl p wird, d. h. es besteht der Satz: Besitzt die Ordnung r einer Gruppe den Primzahlfaktor p, so enthält diese Gruppe einen Operator der Ordnung p; und ebenso gilt folgende, von Sylow herrührende Verallgemeinerung: Ist die Ordnung r einer Gruppe durch die Primzahlpotenz p^α teilbar, so enthält diese Gruppe einen Teiler der Ordnung p^α. An die Beweise dieser Theoreme, die wir im vorliegenden Kapitel behandeln werden, schließen sich naturgemäß die Sätze an, die G. Frobenius erweiternd und ergänzend gegeben hat.

§ 77. Für Abelsche Gruppen gilt die Umkehrung des obigen Satzes in voller Allgemeinheit: Hat die Ordnung r einer Abelschen Gruppe den Faktor n, so enthält die Gruppe auch Teiler der Ordnung n. Nach den Darlegungen von § 66, S. 83 reicht es aus, den Beweis für eine Abelsche Gruppe der Ordnung $r = p^\alpha$ und einen Teiler der Ordnung $n = p^\beta$ $(\beta \leqq \alpha)$ zu führen. Wir betrachten die Darstellung der Operatoren einer solchen Gruppe durch eine Basis (§ 67, S. 86) $a_1, a_2, \ldots, a_\varrho$ in der Gestalt

$$a_1^{\varkappa_1} a_2^{\varkappa_2} \ldots a_\varrho^{\varkappa_\varrho} \qquad (\varkappa_1 = 1, 2, \ldots, p^{n_1};\ \varkappa_2 = 1, 2, \ldots, p^{n_2};\ \ldots)$$
$$(n_1 + n_2 + \ldots + n_\varrho = \alpha).$$

Nun bestimmen wir ϱ Operatoren $b_1, b_2, \ldots, b_\varrho$ durch die Gleichungen

$$b_1 = a_1^{p^\sigma},\ b_2 = a_2^{p^\tau},\ \ldots,\ b_\varrho = a_\varrho^{p^\omega},$$

wobei die Wahl der Exponenten nur der Beschränkung

$$\sigma + \tau + \ldots + \omega = \alpha - \beta$$

unterworfen sein soll. Dann haben $b_1, b_2, \ldots, b_\varrho$ die Ordnungen $p^{n_1-\sigma}, p^{n_2-\tau}, \ldots, p^{n_\varrho-\omega}$; also liefern die Potenzprodukte der $b_1, b_2, \ldots, b_\varrho$ eine Abelsche Gruppe von der Ordnung

$$p^{n_1-\sigma} \cdot p^{n_2-\tau} \cdot \ldots \cdot p^{n_\varrho-\omega} = p^{\alpha-(\alpha-\beta)} = p^\beta;$$

und dies ist eine der Untergruppen, deren Existenz oben behauptet worden war.

§ 78. Wir schieben hier die Herleitung einer von Frobenius gegebenen Hilfsformel ein, deren wir später bedürfen.

G sei eine Gruppe der Ordnung r; H und K, von der Ordnung s bzw. t, seien zwei Teiler von G. Aus G nehmen wir einen beliebigen Operator g, bilden mit g den Komplex HgK, der aus $s \cdot t$ Operatoren besteht und fragen, wieviel verschiedene Operatoren in diesem Komplexe der $s \cdot t$ Operatoren vorkommen. Aus der Annahme der Gleichheit

$$h_1 g k_1 = h_2 g k_2,$$

wo h_1, h_2 Operatoren aus H und k_1, k_2 solche aus K bedeuten, folgt

$$(1)\qquad \begin{cases} g = h_1^{-1} h_2 g k_2 k_1^{-1} = h_0 g k_0 , \\ \qquad g^{-1} h_0 g = k_0^{-1} . \end{cases}$$

Nun gehört die linke Seite der letzten Gleichung zu den Operatoren der Gruppe $g^{-1} H g$ und die rechte zu K; also beide zur Gruppe $L = \}g^{-1} H g, K\{$. Dieses L möge die Ordnung u haben. Dann sind von den $s \cdot t$ Operatoren aus $H g K$ je u einander gleich. Es ergibt sich nämlich umgekehrt für jedes l_α aus der Gruppe L die Relation

$$(h_1 g l_\alpha g^{-1}) g (l_\alpha^{-1} k_1) = h_1 g k_1 ,$$

wobei wegen $g L g^{-1} = \}H, g K g^{-1}\{$ der Operator $g l_\alpha g^{-1}$, also auch $h_1 g l_\alpha g^{-1}$ der Gruppe H, dagegen $l_\alpha^{-1} k$ der Gruppe K angehört. Folglich liefert der Komplex $H g K$ genau $\frac{s t}{u}$ verschiedene Operatoren, und dabei kommt jeder genau u-mal unter den $H g K$ vor.

Ist g' ein nicht in $H g K$ vorkommender Operator, so haben die beiden Komplexe

$$H g K \quad \text{und} \quad H g' K$$

ersichtlich keinen gemeinsamen Operator.

Folglich kann man die Operatoren von G in Klassen verteilen, indem man zwei Operatoren dann und nur dann zu der gleichen Klasse rechnet, wenn sie beide in demselben Komplexe $H g K$ vorkommen. Die Anzahl der Komplexe bei G sei n und die Zerlegung von G in einzelne Klassen liefere

$$G = H g_1 K + H g_2 K + \ldots + H g_n K .$$

Diese Darstellung heißt die Zerlegung von G nach dem Doppelmodul H, K.

Die Klasse, die g_λ enthält, liefert $\frac{s t}{u_\lambda}$ verschiedene Operatoren und zwar einen jeden u_λ mal, wo u_λ die Ordnung der Gruppe

$$L_\lambda = \}g_\lambda^{-1} H g_\lambda , K\{$$

bedeutet.

Setzt man die Ordnung r von G gleich der Summe aus den Anzahlen der Operatoren in den einzelnen Klassen, so entsteht

$$(2)\qquad \begin{cases} \dfrac{s\,t}{u_1} + \dfrac{s\,t}{u_2} + \dots + \dfrac{s\,t}{u_n} = r\,, \\[2ex] \dfrac{1}{u_1} + \dfrac{1}{u_2} + \dots + \dfrac{1}{u_n} = \dfrac{r}{s \cdot t}\,. \end{cases}$$

Dabei ist u_λ seiner Bedeutung nach ein Divisor der Ordnung t von K; wir können daher mit ganzzahligen f_λ

$$(3)\qquad t = f_1 u_1 = f_2 u_2 + \dots = f_n u_n$$

setzen, wo f_λ der Index des Teilers L_λ bezüglich K ist. Führen wir diese Zahlen $f_1, f_2, \dots, f_n$ in (2) ein, so entsteht die Gleichung

$$(4)\qquad f_1 + f_2 + \dots + f_n = \frac{r}{s}\,.$$

§ 79. Ist die Ordnung $r = p^\alpha \cdot \varrho$ der Gruppe G genau durch die αte Potenz der Primzahl p teilbar, so enthält G einen Teiler der Ordnung p^α. (I. Satz von Sylow.)

Wir benutzen die in § 39, S. 56 gegebene Verteilung der Operatoren von G in Transformationskomplexe seiner Operatoren und erhalten für die Ordnung von G die Bestimmung

$$(5)\qquad r = p^\alpha \cdot \varrho = 1 + \sigma_2 + \sigma_3 + \dots + \sigma_\delta + \dots + \sigma_k\,.$$

In dieser Gleichung bezieht sich jedes σ_δ auf einen Operator g_δ von G, und zwar zeigt σ_δ die Anzahl der voneinander verschiedenen Operatoren an, in die g_δ durch sämtliche Operatoren von G transformiert wird, also der voneinander verschiedenen, die $\bar{G}^{-1} g_\delta \bar{G}$ enthält. Daher (S. 54) ist σ_δ der Index der Zwischengruppe J_δ von g_δ in G. Bezeichnen wir mit i_δ die Ordnung von J_δ, so wird $\sigma_\delta = \dfrac{r}{i_\delta}$ und (5) liefert die Gleichung

$$(5\text{a})\qquad r = p^\alpha \varrho = 1 + \frac{r}{i_2} + \frac{r}{i_3} + \dots + \frac{r}{i_k}\,.$$

In G mögen genau h selbstkonjugierte Operatoren

vorkommen, etwa $1, g_2, g_3, \ldots, g_h$; für jeden von diesen g_λ fällt die Zwischengruppe J_λ mit G zusammen, c_λ mit 1 und r mit i_λ. $\{g_2, g_3, \ldots, g_h\}$ ist eine Abelsche Gruppe H.

Faßt man nun in (5a) die Brüche zusammen, die wegen $r = i_\lambda$ den Wert 1 haben, so entsteht die Umformung

$$p^\alpha \varrho = h + \frac{p^\alpha \varrho}{i_{h+1}} + \frac{p^\alpha \varrho}{i_{h+2}} + \cdots + \frac{p^\alpha \varrho}{i_k}. \tag{6}$$

Die hier noch auftretenden i_δ sind eigentliche Teiler von $p^\alpha \cdot \varrho = r$, also $i_\delta < r$.

Nach diesen Vorbereitungen gehen wir zum Beweise des ausgesprochenen Sylowschen Satzes über; wir wollen ihn durch Induktion liefern.

Wir nehmen an erster Stelle an, daß die Ordnung h von H nicht durch p teilbar ist; dann folgt aus (6), daß mindestens einer der auf den ersten Summanden folgenden Brüche rechts zu p teilerfremd sein muß; und das entsprechende i_δ des Nenners enthält dann den Faktor p^α. Daher hat J_δ die Ordnung $p^\alpha \cdot \varrho_0$ mit $\varrho_0 < \varrho$, weil i_δ ein echter Teiler von r ist. Es ist also die Frage auf Gruppen niederer Ordnung zurückgeführt.

Wir nehmen zweitens an, h sei durch eine Potenz von p und zwar genau durch p^β bei $\beta > 0$ teilbar. Für $\beta = \alpha$ wäre H ein Teiler, und da H eine Abelsche Gruppe ist, so wäre nach § 77 der Satz bewiesen. Wir haben daher nur noch den Fall $\beta < \alpha$ zu betrachten. Die Abelsche Gruppe H in G hat also eine, genau durch p^β teilbare Ordnung ($\beta < \alpha$). H ist in G selbstkonjugiert; folglich kann man die Faktorgruppe $G/H = \Gamma$ bilden. Diese Gruppe ist isomorph zu G und ihre Ordnung $= p^{\alpha-\beta} \varrho_0$; der Isomorphismus von G zu Γ ist p^β-stufig. Gilt unser Satz für Γ, dann folgt, daß G einen Teiler der Ordnung $p^{\alpha-\beta} \cdot p^\beta = p^\alpha$ hat (§ 30, S. 44).

Das Theorem ist demnach bewiesen, wenn es für Gruppen der Ordnung

$$p^\alpha \varrho' \quad \text{oder} \quad p^\beta \varrho_0 \qquad (\varrho' < \varrho\,;\ \beta < \alpha)$$

richtig ist.

Gelangt man aber bei den obigen beiden Reduktionen auf $\varrho_0 = 1$‘ so ist der Satz klar; gelangt man auf $\beta = 0$,

ebenfalls. Damit ist die Richtigkeit des Theorems nachgewiesen.

§ 80. Nachdem so dargetan ist, daß G einen Teiler H der Ordnung p^α hat, wenn p^α die höchste in r aufgehende Potenz der Primzahl p ist, nehmen wir an, es gebe in G noch einen anderen Teiler K der gleichen Ordnung $t = p^\alpha$. Wir wenden auf G, H, K die Formel (4) aus § 78 an:

$$f_1 + f_2 + \ldots + f_n = \frac{r}{s} = \frac{p^\alpha \varrho}{p^\alpha} = \varrho ,$$

wo ϱ teilerfremd zu p ist. Jedes f_λ ist ein Teiler von $t = p^\alpha$, also selbst eine Potenz von p. Folglich muß mindestens eins der f_λ den Wert 1, und der zugehörige Bruch

$$\frac{t}{f_\lambda} = u_\lambda ,$$

d. h. die Ordnung von $\}g_\lambda^{-1} H g_\lambda , K\{$ den Wert $t = p^\alpha$ haben. Nun ist $t = p^\alpha$ die Ordnung von K; also wird K in $g_\lambda^{-1} H g_\lambda$ enthalten sein. Der gleichen Ordnungen halber folgt daher

$$K = g_\lambda^{-1} H g_\lambda ,$$

d. h. K ist eine Transformierte von H. So kommen wir auf das folgende Resultat: Alle Teiler H der Ordnung p^α von G bilden ein einziges konjugiertes System, d. h. alle können durch $\bar{G}^{-1} H \bar{G}$ aus einem beliebigen unter ihnen hergeleitet werden. (II. Satz von Sylow.)

§ 81. Wir betrachten jetzt die Zwischengruppen J_λ der H_λ in G. Die H_λ sind die Teiler der Ordnung p^α in G von der Ordnung $p^\alpha \cdot \varrho$, wo ϱ teilerfremd zu p ist. Die Ordnung von J_λ ist ein Vielfaches von p^α und ein Teiler von $p^\alpha \varrho$. Die Ordnungen von $J_1, J_2, J_3, \ldots$ sind einander gleich, wie aus den Resultaten des vorigen Paragraphen erhellt, daß die $H_1, H_2, H_3, \ldots$ zueinander konjugiert sind. Die Ordnung von H_1 sei $p^\alpha \cdot m$, ferner sei $\varrho = m \cdot m_1$, also $r = p^\alpha m m_1$. Die Zwischengruppe J_λ kann nur eine einzige Gruppe H_λ des Transformationskomplexes

$$\bar{G}^{-1} H_\lambda \bar{G}$$

enthalten. Käme nämlich in J_λ noch ein zweites H_μ vor, so wäre, weil J_λ alle und nur die mit H_λ vertauschbaren Operatoren von G enthält, $J_\lambda^{-1} H_\lambda J_\lambda = H_\lambda$, also auch

$$\bar{H}_\mu^{-1} H_\lambda \bar{H}_\mu = H_\lambda \quad \text{und} \quad H_\lambda H_\mu = H_\mu H_\lambda ;$$

bezeichnen wir die Ordnung von $\}H_\lambda, H_\mu\{$ mit p^β, so ist die Ordnung von $\{H_\lambda, H_\mu\}$ nach § 40, S. 57 gleich

$$(p^\alpha \cdot p^\alpha) : p^\beta = p^{2\alpha-\beta} .$$

Da $\{H_\lambda, H_\mu\}$ ein Teiler von G ist, und da G die Ordnung $p^\alpha \cdot \varrho$ hat, so muß $\beta = \alpha$ werden, d. h. H_λ fällt mit H_μ zusammen.

Damit ist zugleich auch bewiesen: Jede der konjugierten Gruppen H_λ kommt nur in einer der konjugierten Zwischengruppen J_λ vor. Denn wäre z. B. H_λ gleichzeitig in J_λ und in $J_\mu = g_0^{-1} J_\lambda g_0$ enthalten, so enthielte $g_0^{-1} J_\lambda g_0$ außer H_λ noch $g_0^{-1} H_\lambda g_0$. Das ist aber $\neq H_\lambda$, da g_0 nicht zu J_λ gehört. Das widerspräche dem zuerst bewiesenen Satze.

Nun wenden wir die Formel (4), § 78 derart an, daß wir die dortigen Bezeichnungen

$$G, H, K; \quad r, s, t$$

jetzt durch

$$G, J, H; \quad p^\alpha m m_1, \; p^\alpha m, \; p^\alpha$$

ersetzen. Die Ordnung u_λ der Gruppe $\}g_\lambda^{-1} J g_\lambda, H\{$ ist ein Teiler der Ordnung von H, d. h. von p^α. Diese wird für $g_\lambda = 1$ zu $u_\lambda = p^\alpha$; für jedes andere g_λ, das nicht in J enthalten ist, folgt $u_\lambda < p^\alpha$, da H nicht auch ein Teiler von $g_\lambda^{-1} J g_\lambda$ sein kann. Daher wird eins der f_λ gleich 1, die anderen dagegen werden von 1 verschiedene Potenzen von p. Somit liefert (4) § 78

$$1 + p^\gamma + p^\delta + \ldots = \frac{r}{s} = m_1 = 1 + p k$$

oder

$$r = p^\alpha m (1 + p k) . \tag{7}$$

So kommen wir auf das weitere Resultat:

Die Anzahl der Gruppen H der Ordnung p^α, die in G enthalten sind, ist kongruent 1 modulo p;

denn jeder der m_1 Gruppen J_λ entspricht eine Gruppe H_λ. (III. Satz von Sylow.)

§ 82. Frobenius hat weiter nachgewiesen: Ist n ein Teiler der Ordnung r einer Gruppe, so ist die Anzahl der Operatoren dieser Gruppe, deren Ordnung in n aufgeht, ein Vielfaches von n. Alle diese Operatoren können auch dadurch gekennzeichnet werden, daß sie der Gleichung $x^n = 1$ genügen, daß also die $n$te Potenz eines jeden gleich dem Einheitsoperator wird.

Wir betrachten beispielsweise die Gruppe 6ter Ordnung (5) aus § 17, S. 27

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	f	e	a	c	b
e	e	d	f	b	a	c
f	f	e	d	c	b	a.

In ihr sind von der ersten, zweiten, dritten Ordnung bzw. die Operatoren

$$a; \quad d, e, f; \quad b, c,$$

und es genügen daher den Gleichungen

$x^1 = 1$ der Operator a;
$x^2 = 1$ die Operatoren a, d, e, f;
$x^3 = 1$ die Operatoren a, b, c.

Hier weist sich daher der Satz als richtig aus; das gleiche findet offenbar für alle Gruppen von Primzahlordnung statt. Auch für zyklische Gruppen ist er gültig; denn handelt es sich um $G = \{g\}$ mit $g^r = 1$ als niedrigster Potenz, die dem Einheitsoperator gleich wird, so hat für den Teiler n von r die Gleichung

$$x^n = 1$$

als Lösungen die n Operatoren

$$x = g^{r:n}, \; g^{2r:n}, \; g^{3r:n}, \; \ldots, \; g^{nr:n},$$

und nur diese.

Den Beweis für den allgemeinen Satz führen wir durch strenge Induktion. Wir nehmen an, der Satz sei für alle Gruppen richtig, deren Ordnung $r' < r$ ist; und bei den Gruppen der Ordnung r für alle Teiler, deren Ordnung $n' > n$ ist. Diese letzte Annahme dürfen wir machen, da das Theorem für $n = r$ klar ist.

Es sei nun eine Gruppe G der Ordnung r vorgelegt; n soll ein eigentlicher Teiler von r, also $n < r$ sein. Der Bruch $\frac{r}{n}$ möge den Primfaktor p haben, und n sei $= p^{\lambda-1} \cdot s$, wo s teilerfremd zu p ist; r ist demnach durch p^λ teilbar. Nach der zweiten Annahme ist die Anzahl der Wurzeln von $x^{np} = 1$ ein Vielfaches von np, also von n. Kann gezeigt werden, daß die Anzahl derjenigen von diesen Operatoren, die nicht schon $x^n = 1$ befriedigen, auch ein Vielfaches von n ist, so muß die Anzahl der übrig bleibenden, d. h. aller, die da Wurzeln von $x^n = 1$ sind, auch ein Vielfaches von n sein. Damit wäre also der Beweis des Satzes geliefert.

Den Komplex dieser Operatoren, für die

$$x^n \neq 1 \quad \text{aber} \quad x^{np} = 1 \tag{8}$$

wird, bezeichnen wir mit K und weisen nach, daß die Anzahl der zu K gehörenden Operatoren sowohl durch $p^{\lambda-1}$ wie auch durch s teilbar ist; denn dann ist ihre Anzahl auch durch $n = p^{\lambda-1} \cdot s$ teilbar, da p und s teilerfremd sind.

I. Die Anzahl der Operatoren von K ist durch $p^{\lambda-1}$ teilbar. Beweis: Die Ordnung jedes Operators k_ϱ von K ist wegen (8) ein Teiler von $np = p^\lambda s$, aber kein Teiler von $n = p^{\lambda-1} s$. Also ist jede solche Ordnung $= p^\lambda s_\varrho$, wo s_ϱ einen Teiler von s bedeutet. Wir teilen nun die Operatoren k_ϱ von K in Klassen ein, indem wir zwei Operatoren dann und nur dann zur gleichen Klasse rechnen, wenn jeder eine Potenz des anderen ist. Dann gehören zur Klasse eines k_ϱ die und nur die Potenzen von k_ϱ, deren Exponenten teilerfremd zur Ordnung von k_ϱ sind, d. h. zu $p^\lambda s_\varrho$. Das sind der Zahl nach, wenn φ die bekannte zahlentheoretische Funktion bedeutet, $\varphi(p^\lambda s_\varrho)$ Operatoren, also ein Vielfaches von $p^{\lambda-1}$. Da jeder Operator nur einer Klasse angehört, so ist, wie be-

wiesen werden sollte, die Anzahl aller Operatoren von K ein Vielfaches von $p^{\lambda-1}$.

II. Die Anzahl der Operatoren von K ist durch s teilbar. Beweis: Die Ordnung jedes Operators k_ϱ aus K ist $p^\lambda s_\varrho$, wo s_ϱ ein Divisor von s, also teilerfremd zu p ist. Nach § 15, S. 18 ist jedes k_ϱ auf eine und nur eine Art als ein Produkt $a_\varrho \cdot b_\varrho$ darstellbar, bei dem a_ϱ die Ordnung p^λ, b_ϱ die Ordnung s_ϱ hat, a_ϱ und b_ϱ miteinander vertauschbar sind. Folglich kommt $k_\varrho = a_\varrho b_\varrho$ in der zu dem Operator a_ϱ gehörigen Zwischengruppe J_ϱ vor. (Um Jrrtümern zu begegnen, heben wir hervor, daß J_ϱ nicht die Zwischengruppe zu dem Teiler $\{a_\varrho\}$ ist. Diese ist allgemeiner; die zu ihr gehörigen Operatoren dürfen a_ϱ in eine Potenz $a_\varrho^\varkappa$ transformieren; unser J_ϱ dagegen transformiert a_ϱ in sich selbst.)

Sucht man daher alle a_ϱ auf, d. h. alle Operatoren der Ordnung p^λ in G, und bestimmt für jedes dieser a_ϱ die Gruppe J_ϱ aller mit a_ϱ vertauschbaren Operatoren, so enthalten die so bestimmten J_ϱ alle Operatoren von K und zwar jedes $k_\varrho = a_\varrho b_\varrho$ nur einmal, da a_ϱ und b_ϱ durch das k_ϱ eindeutig bestimmt sind, § 15, S. 18.

Wir betrachten deshalb ein $k_\varrho = a_\varrho b_\varrho$ und die Gruppe J_ϱ. Der Kürze wegen unterdrücken wir den Index ϱ. Die Ordnung von J, die ein Vielfaches der Ordnung von a ist, möge $p^\lambda t$ sein. Die Ordnung jedes k ist ein Teiler von $p^\lambda s$. Also ist die Ordnung jedes in unserem J vorkommenden k gleichzeitig Teiler von $p^\lambda s$ und von $p^\lambda t$, also von $p^\lambda u$, wenn u den größten gemeinsamen Divisor von s und t bedeutet. Alle k, die in J auftreten, sind demnach Wurzeln der Gleichung $x^{p^\lambda \cdot u} = 1$.

Nun ist die Anzahl derjenigen Operatoren b in J zu bestimmen, die bei der erwähnten Zerfällung von k in $a \cdot b$ ein b liefern, das der Gleichung $x^u = 1$ genügt.

Da $\{a\}$ selbstkonjugiert in J ist, so gibt es eine Faktorgruppe $\Gamma = J/\{a\}$, zu der J in p^λ-stufigem Isomorphismus steht. Die Konstitution dieser Gruppe entnehmen wir aus der Darstellung

$$(9) \qquad \begin{cases} J = \{a\} + c_2\{a\} + c_3\{a\} + \dots + c_t\{a\} \\ \quad = \gamma_1 + \gamma_2 + \gamma_3 + \dots + \gamma_t, \end{cases}$$

indem wir die $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_t$ als Operatoren von Γ auffassen und γ_1 den Einheitsoperator in Γ bedeuten lassen. Weil die Ordnung von Γ niedriger ist als die von G, so gilt nach der ersten Annahme für Γ und die Teilerordnung u der zu beweisende Satz. Es gibt somit $u \cdot v$ Operatoren in Γ, deren Ordnung ein Teiler von u ist, so daß sie die Gleichung $x^u = 1$ befriedigen. Sei γ_α ein solcher, für den also $\gamma_\alpha^u = \gamma_1$ wird, dann muß wegen des Isomorphismus die $u$te Potenz jedes Operators aus dem Komplexe $c_\alpha\{a\}$ zu dem Komplexe $\{a\}$ gehören; insbesondere wird c_α^u gleich einer Potenz von a, etwa $= a^\omega$, sein für jedes $\alpha = 2, 3, \ldots, t$. Nun läßt sich c_α in zwei Faktoren zerlegen, $c_\alpha = a'_\alpha \cdot b'_\alpha$, die miteinander vertauschbar sind, und von denen a'_α als Ordnung eine Potenz von p hat, während die Ordnung von b'_α zu p teilerfremd ist. Wegen der Vertauschbarkeit ist

$$c_\alpha^u = (a'_\alpha b'_\alpha)^u = (a'_\alpha)^u (b'_\alpha)^u = a^\omega ,$$

und wegen der Eindeutigkeit der Zerlegung treten die Beziehungen ein

$$(a'_\alpha)^u = a^\omega ; \quad (b'_\alpha)^u = 1 .$$

Da u zu p teilerfremd ist, so zeigt das erste dieser Resultate, daß a'_α selbst gleich einer Potenz von a wird, $a'_\alpha = a^\pi$; also hat man in (9) für J die Summandenumformung

$$c_\alpha\{a\} = a'_\alpha b'_\alpha\{a\} = b'_\alpha a'_\alpha\{a\} = b'_\alpha\{a\} \qquad (\alpha = 2, 3, \ldots, t) .$$

In diesem Komplexe ist b'_α der einzige Operator, dessen $u$te Potenz $= 1$ wird; für alle anderen $b'_\alpha a^\varrho$ ist die Ordnung eine höhere, weil durch p teilbare. Daraus sieht man, daß (9) in J wie in Γ genau $u \cdot v$ Operatoren hat, die $x^u = 1$ befriedigen. Sind das die Operatoren $b'_2, b'_3, \ldots$, so sind $a b'_2, a b'_3, \ldots$ die sämtlichen und die einzigen in J vorhandenen und in G zu a gehörigen k. Es gibt daher von diesen genau $u \cdot v$ in J, die bei der erwähnten Zerlegung den Operator a als Faktor der Ordnung p^λ und den Operator b als Faktor der Ordnung u aufweisen.

Transformiert man J durch sämtliche Operatoren von G, so entstehen $\frac{r}{p^\lambda \cdot t}$ zu J konjugierte Gruppen und

ebenso viele Systeme k von je $u \cdot v$ Operatoren; also zusammen $\frac{r u v}{p^\lambda t}$. Die Zahl r ist durch $p^\lambda \cdot s$ und durch $p^\lambda \cdot t$ teilbar; demnach durch $(p^\lambda s \cdot p^\lambda t) : (p^\lambda u) = \frac{p^\lambda s t}{u}$, also $r \cdot u$ durch $p^\lambda s t$. Um so mehr ist $\frac{r u v}{p^\lambda t}$ ein Vielfaches von s. Die so aus a erhaltenen Operatoren ordnen wir in ein System, dessen Ordnung nach dem Bewiesenen durch s teilbar ist. Das System ist durch jeden zugehörigen Operator k vollständig bestimmt, so daß zwei verschiedene Systeme keinen Operator gemeinsam haben. Mithin ist die Summe der Operatoranzahlen aller Systeme durch s teilbar.

Damit ist auch der zweite Teil des aufgestellten Satzes bewiesen.

Weil der Einheitsoperator der Forderung $x^n = 1$ genügt, ist die Anzahl aller Operatoren von G, die $x^n = 1$ befriedigen, ein von Null verschiedenes Vielfache von n.

§ 83. Frobenius hat Erweiterungen seines Theorems gefunden, von denen wir, ohne auf die nicht allzu leichten Beweise einzugehen, die Hauptsache angeben wollen.

Wir schicken folgende Definition voraus: Gehören die Operatoren des Komplexes

$$K = [g_1, g_2, g_3, \cdots, g_{r_1}]$$

sämtlich zur Gruppe

$$G = \{g_1, g_2, g_3, \cdots, g_{r_1}, g_{r_1+1}, \cdots, g_r\},$$

und ist für jedes g_α der Gruppe G

$$\overline{G}^{-1} K \overline{G} = g_\alpha^{-1} K g_\alpha = [g_\alpha^{-1} g_1 g_\alpha, \cdots, g_\alpha^{-1} g_{r_1} g_\alpha] = K,$$

so heißt K ein in G selbstkonjugierter Komplex.

Dann beweist Frobenius den Satz:

Bilden die r_1 Operatoren

$$g_1, g_2, g_3, \cdots, g_{r_1}$$

in der Gruppe G von der Ordnung r einen selbstkonjugierten Komplex, so ist die Anzahl der Operatoren von G, die einer der Gleichungen

$$x^n = g_1, \quad x^n = g_2, \quad x^n = g_3, \quad \cdots, \quad x^n = g_{r_1}$$

genügen, durch den größten gemeinsamen Teiler von r und n teilbar. Diese Anzahl kann hier auch gleich Null sein, während die entsprechende Anzahl bei dem Satze des vorigen Paragraphen von Null verschieden war. Der jetzige Satz geht in den vorigen über, wenn man $K = 1$ setzt und für n einen Teiler von r nimmt.

§ 84. Auch über den Fall, daß die Operatoren von G, deren Ordnung ein Teiler von n ist, nicht nur als Vielfaches von n, sondern genau in der Anzahl n vorhanden sind, hat Frobenius ein Theorem gegeben, von dem wir später noch Nutzen ziehen werden. Es lautet: Sind die Primfaktoren der Zahl a alle untereinander verschieden, und ist jeder Primfaktor von b größer als der größte Primfaktor von a, so gibt es in jeder Gruppe der Ordnung ab genau b Operatoren, deren Ordnung in b aufgeht. Auch diesen Satz beweist er wie den vorigen durch strenge Induktion.

Wir nehmen an, der Satz gelte für alle Gruppen, deren Ordnung $a_1 \cdot b_1 < a \cdot b$ ist, und für die Gruppen mit der Ordnung $a \cdot b$, sobald die Anzahl der in a aufgehenden Primfaktoren $<n$ ist. Dann zeigen wir seine Richtigkeit auch bei a und b für n Primfaktoren von a. Da er für $a_1 = 2$, $b_1 = 3$ und bei jeder Ordnung ab für $a = 1$ also $n = 0$ richtig ist, so reicht dieser Nachweis aus, um die Gültigkeit des Theorems allgemein darzutun.

Schreiben wir die Ordnung $a \cdot b$ der Gruppe G in der Form $\frac{a}{p} \cdot pb$, wo p der größte Primfaktor von a ist, so besitzt nach dem als richtig vorausgesetzten Satze G genau $p \cdot b$ Operatoren, die der Gleichung $x^{p \cdot b} = 1$ genügen; denn $\frac{a}{p}$ enthält weniger Primfaktoren als a. Von diesen $p \cdot b$ Operatoren schalten wir die aus, deren Ordnung ein Vielfaches von p ist; dann bleiben alle und nur die zurück, deren Ordnung gleich b oder gleich einem Teiler von b ist, also gerade die, deren Anzahl wir bestimmen wollen. Wir untersuchen daher den Komplex K der Operatoren $\varkappa$, deren Ordnung ein Vielfaches von p und ein Teiler von $p \cdot b$ ist. Die Operatoren $\varkappa$ sind unter den Operatoren γ enthalten, deren Ordnung q ein Vielfaches von p ist. Ist γ einer von ihnen und $q = r \cdot p$ seine Ordnung, so ist γ^r von der

Ordnung p. Die Operatoren der Ordnung p wollen wir mit π bezeichnen. Da γ mit $\gamma^r = \pi$ vertauschbar ist, so gehört γ zur Zwischengruppe J von $\{\pi\}$ in G. Bildet man daher alle Gruppen $\{\pi\}$ und zu jeder die zugehörige Zwischengruppe J, so sind alle γ und damit alle $\varkappa$ in den J enthalten. Die $\varkappa$ verteilen sich also in die einzelnen J. Jedes $\varkappa$ tritt nur in einem J auf, da durch ein γ, also auch ein $\varkappa$, der Operator $\pi = \gamma^r$ eindeutig bestimmt ist. Wir werden nun sofort beweisen, daß alle J gleichviele $\varkappa$ enthalten. Folglich braucht man nur zu bestimmen, zunächst wie viele Gruppen J es gibt, und zweitens wie viele $\varkappa$ in einem (also in jedem) J vorkommen. Das Produkt beider Zahlen liefert die gesuchte Gesamtanzahl der $\varkappa$, also das, was wir suchen.

Wir bestimmen zunächst die Anzahl der J. Da p als Primfaktor von a der Annahme nach nur in der ersten Potenz in $a\,b$ vorkommt, so hat G Teiler der Ordnung p, aber keine der Ordnung p^2. Diese Teiler der Ordnung p gehören sämtlich zu demselben konjugierten Systeme, ebenso wie die zugehörigen Zwischengruppen (§ 80, S. 103). Es sei $\{\pi\}$ ein solcher Teiler der Ordnung p; seine Zwischengruppe J habe die Ordnung $a'p\,b'$, wobei $a = a'a''p$ und $b = b'b''$, also $a'p$ ein Divisor von a und b' ein solcher von b ist. Dann folgt, daß G genau $a'' \cdot b''$ Gruppen J enthält; da diese einander konjugiert sind, so enthalten sie je gleich viele Operatoren $\varkappa$. Damit ist die am Schlusse des vorigen Absatzes ausgesprochene Behauptung bewiesen und die Anzahl der J gleich $a''b''$ festgestellt.

Wir bestimmen zweitens die Anzahl der $\varkappa$ in einem J. Der Definition nach hat $\varkappa$ zur Ordnung einen Teiler von $p \cdot b$; da ferner $\varkappa$ in J vorkommt, so hat $\varkappa$ zur Ordnung einen Teiler von $a'p\,b'$; also ist die Ordnung von $\varkappa$ ein Teiler von $p \cdot b'$ und zugleich nach der Definition ein Vielfaches von p. Die $\varkappa$ kommen folglich in J unter den Operatoren vor, deren Ordnung q in $p \cdot b'$ aufgeht; wir bezeichnen diese durch η. Die Anzahl der η in J ist gleich $p\,b'$; denn J hat die Ordnung $a'p\,b'$, die im allgemeinen $< a\,b$ ist; und im besonderen Falle $a'p\,b' = a\,b$ hat a' weniger Primfaktoren als $a = a'a''p$. In beiden Fällen kommen wir auf die Voraussetzungen unseres In-

duktionsschlusses und ersehen, daß J genau $p\,b'$ Operatoren η einschließt. Mit η haben zugleich die Operatoren

(10) $$\eta\,,\ \eta\,\pi\,,\ \eta\,\pi^2,\ \ldots,\ \eta\,\pi^{p-1}$$

die charakteristische Eigenschaft des η, daß ihre Ordnung in $p\,b'$ aufgeht. Denn η ist mit $\{\pi\}$ vertauschbar, da es zu J gehört; und somit

$$(\eta\,\pi^a)^{p\,b'} = \eta^{p\,b'}(\pi^c)^{p\,b'} = 1\ .$$

Demnach verteilen sich die $b\,p'$ Operatoren η von J in b' Komplexe (10) von je p Operatoren. Es soll nun bewiesen werden, daß jeder dieser Komplexe (10) genau $(p-1)$ Operatoren $\varkappa$ enthält; d. h. daß in jedem Komplexe (10) $(p-1)$ Operatoren vorkommen, deren Ordnung durch p teilbar ist, und einer, dessen Ordnung nicht durch p teilbar ist.

Zu diesem Zwecke zeigen wir zuerst, daß η nicht nur mit $\{\pi\}$, sondern sogar mit π selbst vertauschbar ist. Aus

$$\eta^{-1}\,\pi\,\eta = \pi^s \quad \text{folgt} \quad \eta^{-\alpha}\,\pi\,\eta^\alpha = \pi^{s^\alpha}$$

und für $\alpha = q$, da q die Ordnung von η bedeutet,

$$\eta^{-q}\,\pi\,\eta^q = \pi = \pi^{s^q}\ ; \quad s^q \equiv 1 \pmod{p}\ .$$

Andererseits ist nach dem F e r m a t schen Satze auch $s^{p-1} \equiv 1 \pmod{p}$. Nun ist q ein Teiler von $p\,b'$, also teilerfremd zu $(p-1)$, da alle Primfaktoren von b größer als p sind. Die beiden letzten Kongruenzen liefern daher $s = 1$ und $\eta\,\pi = \pi\,\eta$.

Ist jetzt zunächst q, d. h. die Ordnung von η, nicht durch p teilbar, dann gehört η nicht zu den $\varkappa$, dagegen jedes der weiteren $\eta\,\pi^h$; denn die Operatoren haben für jedes $h \neq 0$ eine durch p teilbare Ordnung.

Ist dagegen $q = r\,p$, so hat η^r die Ordnung p, ist also eine Potenz von π, etwa $\eta^r = \pi^s$; und wenn t durch die Kongruenz

$$s\,t \equiv 1 \pmod{p}$$

bestimmt und $r\,t = u$ gesetzt wird, $\eta^u = \pi$. Dadurch geht (10) in

(10a) $$\eta\,,\ \eta^{u+1},\ \eta^{2u+1},\ \ldots,\ \eta^{(p-1)u+1}$$

über. Ist nun v die Ordnung von η^{hu+1}, dann muß

$$v(h\,u + 1) = r\,t\,v\,h + v \quad \text{durch} \quad q = r\,p$$

also v durch r teilbar sein, $v = r\,l$. Das liefert die Bedingung

$$l(h\,u + 1) \equiv 0 \pmod{p} \qquad (v \min)$$

und fordert $l \equiv 0$, d. h. v wird ein Vielfaches von p, sobald nicht $h\,u + 1 \equiv 0$. Aber diese Kongruenz modulo p hat nur eine Wurzel $h = h_0$. Demnach hat $\eta^{h_0 u + 1}$ eine durch p nicht teilbare Ordnung; die Ordnung jedes anderen Operators aus (10a) ist dagegen durch p teilbar. Sonach enthält (10a) wie (10) genau $(p-1)$ Operatoren $\varkappa$.

Die b' Komplexe (10) enthalten zusammen $b'(p-1)$ Operatoren $\varkappa$; alle J zusammen $a''b'' \cdot b'(p-1) = a'' \cdot b(p-1)$. Das ist die Anzahl der $\varkappa$ in G; ihr Ausdruck läßt sich noch vereinfachen. Die Gruppe G enthält nämlich $p\,b$ Operatoren, deren Ordnung in $p\,b$ aufgeht; zu diesen Operatoren gehören die $\varkappa$; ferner gehört zu ihnen die Einheit, die in den $\varkappa$ nicht vorkommt. Folglich ist $p\,b > a''b(p-1)$, daher $(a''-1)(p-1) < 1$, also $a'' = 1$. Sonach enthält G genau $(p-1) \cdot b$ Operatoren $\varkappa$, d. h. $(p-1) \cdot b$ Operatoren, deren Ordnung ein Vielfaches von p und ein Teiler von $p \cdot b$ ist. Ferner gibt es $p\,b$ Operatoren, deren Ordnung ein Teiler von $p\,b$ ist; folglich genau $p\,b - (p-1)\,b = b$, deren Ordnung in b aufgeht.

§ 85. Wir benutzen jetzt die Sylowschen Sätze zur Aufstellung aller Gruppen von der Ordnung $p \cdot q$, wo p und q Primzahlen bedeuten. Da wir früher § 63, S. 80 bereits die Gruppen der Ordnung p^2 aufgestellt haben, so können wir jetzt $p \neq q$ und $p < q$ annehmen. Dann enthält die Gruppe G der Ordnung $p \cdot q$ einen Teiler H der Ordnung q. Nach der Formel (7) § 81, S. 104 ist

$$p \cdot q = q\,m \cdot (1 + \varrho\,q)\,,$$

wo $q\,m$ die Ordnung der Zwischengruppe J von H in G bedeutet. Nun wird bei $k > 0$ der Faktor $(1 + \varrho\,q) > q > p$; also ist $\varrho = 0$ und $m = p$, d. h. H ist ein selbstkonjugierter Teiler von G. Wir setzen $H = \{h\}$, wo h ein Operator der Ordnung q ist.

Zufolge des Cauchyschen Satzes kommt in G auch ein Teiler $K = \{k\}$ der Ordnung p vor. Zunächst nehmen wir an, auch K wäre in G selbstkonjugiert. Dann sind H und K miteinander vertauschbar, und da sie teilerfremd sind, so ist

$$G = \{H, K\} = \{h, k\}\,.$$

Führt man einen Operator $g = h \cdot k$ ein, so folgt leicht $G = \{g\}$, d. h. G ist eine zyklische Gruppe.

Wir betrachten den zweiten möglichen Fall, daß K nicht selbstkonjugiert in G ist. Die Formel (7) § 81, S. 104 gibt hier

$$p \cdot q = p\, m_1(1 + \varrho_1\, p)$$

mit nichtverschwindendem ϱ_1. Dann wird $m_1 = 1$ und $q_1 \equiv 1 \pmod{p}$. Dieser Fall kann also nur für $q = \varrho_1\, p + 1$ eintreten. Der Operator k muß H in sich selbst transformieren, denn H ist selbstkonjugiert in G. Somit ist

$$k^{-1}\, H\, k = H\,, \quad k^{-1}\, h\, k = h^{\alpha}\,,$$

und daraus folgt

$$k^{-p}\, h\, k^{p} = h = h^{\alpha^p}\,,$$

so daß

$$\alpha^p \equiv 1 \pmod{q}\,.$$

Wäre $\alpha = 1$, so hätte man $h\,k = k\,h$; daraus könnten wir wieder die Vertauschbarkeit von H und K erschließen, kämen also auf den schon behandelten Fall. Für α muß daher eine primitive Wurzel der letzten Kongruenz genommen werden, um einen neuen Gruppentypus zu erlangen. Besteht daher eine Gruppe G, so ist sie durch die Vorschriften

$$k^p = 1\,,\ h^q = 1\,; \quad h\,k = k\,h^{\alpha} \qquad (p\,,\ q \min)$$

definiert, wo α eine primitive Wurzel von $\alpha^p \equiv 1 \pmod{q}$ ist. Wie oben, so schließen wir hier wieder, daß die Ordnung der Gruppe $= p \cdot q$ wird. Aus

$$h\,k = k\,h^{\alpha} \quad \text{folgt} \quad h^{\mu}\, k^{\nu} = k^{\nu}\, h^{\mu\,\alpha^{\nu}}\,;$$

daraus ergibt sich leicht das Bestehen des assoziativen Gesetzes und damit das der Gruppe G selbst.

Hätte man statt α eine andere primitive Wurzel der Kongruenz $\alpha^p \equiv 1 \pmod{q}$ genommen, etwa β, so würde eine Gruppe durch die Bestimmungen

$$k^p = 1\,,\ h^q = 1\,; \quad h\,k = k\,h^{\beta} \qquad (p\,,\ q \min)$$

definiert. Nun kann man $\beta^{\tau} \equiv \alpha \pmod{q}$ setzen; es wird dabei

$$h\,k^{\tau} = k^{\tau}\, h^{\alpha}\,,$$

und wenn man $k^{\tau} = k_1$ bezeichnet, dann gehen die obigen Bestimmungen über in

$$k_1^p = 1\,,\ h^q = 1\,;\quad h\,k_1 = k_1\,h^{\alpha} \qquad (p\,,\,q\,\text{min})$$

Demnach ist die mit β gebildete Gruppe der mit α gebildeten einstufig isomorph; wir erlangen somit nur einen neuen Gruppentypus, wie auch α gewählt werde.

Während die Gruppen des ersten Typus Operatoren der Ordnung $p \cdot q$ haben, findet das bei dem zweiten Typus nicht statt. In der Tat, man hat im zweiten Falle

$$(k^{\nu}\,h^{\mu})^{\sigma} = k^{\nu\sigma}\,h^{\mu(\alpha^{\sigma\nu}-1):(\alpha^{\nu}-1)}\,.$$

Ist $\nu = 0$, $\mu \geqq 0$, so ist es klar, daß die Ordnung des Operators gleich q bzw. gleich 1 wird. Ist $\nu > 0$, so muß wegen des ersten Faktors der rechten Seite die Ordnung ein Vielfaches von p sein; aber schon $\sigma = p$ macht $\alpha^p - 1 \equiv 0 \pmod{q}$. Somit wird die Ordnung des Operators gleich p selbst.

---

8. Kapitel.

Auflösbare Gruppen.

§ 86. Es läßt sich eine enge Beziehung zwischen jeder algebraischen Gleichung und einer gewissen, aus ihren Wurzeln als Elementen gebildeten Substitutionengruppe feststellen. Diese Gruppe nennt man die Gruppe der Gleichung. Aus ihrer Natur läßt sich beispielsweise erkennen, ob die Gleichung reduktibel oder irreduktibel ist; ob sie als Eliminationsresultat einer Unbekannten aus zwei Gleichungen aufgefaßt werden kann; ob sie sich mit Hilfe von Wurzeln auflösen läßt. Ist das letzte der Fall, so heißt die Gruppe der Gleichung eine auflösbare Gruppe. Das Charakteristische auflösbarer Gruppen liegt in folgendem: Eine Substitutionengruppe ist auflösbar, wenn ihre Zahlfaktoren der Zusammensetzung sämtlich Primzahlen sind. Da nun die Zahlfaktoren der Zusammensetzung sich bei dem Übergange von einer Gruppe zu einer einstufig isomorphen nicht ändern, so können und wollen wir die gegebene Definition

auflösbarer Gruppen auch bei abstrakten Gruppen anwenden, also den beschränkenden Begriff einer Substitutionengruppe fallen lassen. Die so gekennzeichneten Gruppen sollen jetzt näher untersucht werden.

§ 87. Nun seien G, H die ersten Glieder der Kompositionsreihe von G und die Primzahl p der zugehörige Zahlfaktor. s sei ein Operator aus G, der nicht in H vorkommt. Da die Ordnung von G $p$mal größer ist als die von H, so gibt es keinen echten Teiler von G, der H als echten Teiler enthielte; also ist

$$G = \{H, s\}.$$

Da andererseits $s^{-1} H s = H$ ist, so hat nach § 36, S. 54 $\{H, s\}$ als Ordnung das Produkt der Ordnung von H in den niedrigsten Exponenten k, der s^k zu einem Operator von H macht. Also wird s^p die niedrigste Potenz des Operators s werden, die in dem Teiler H der Gruppe G vorkommt.

Wir wollen nun umgekehrt annehmen, es gebe in G einen Operator s, für den bei einem Teiler H die Beziehung gilt $s^{-1} H s = H$, und dessen $p$te Potenz die erste in H vorkommende ist $\{H, s^p\} = H$; dann erkennt man, daß $\{H, s\} = G$ eine $p$fach so hohe Ordnung hat wie H, und daß H mit dem Kompositionsfaktor p ein Glied der Kompositionsreihe von G wird. Das folgt aus § 36, S. 54.

Wenden wir die angestellten Betrachtungen auf alle Glieder der Kompositionsreihe an, so ergibt sich:

Jede auflösbare Gruppe G ist durch eine Reihe von Operatoren

$$1, s_2, s_3, \ldots, s_\nu$$

bestimmt

$$G = \{s_2, s_3, \ldots, s_\nu\},$$

wobei die s_α folgende beiden Eigenschaften haben: I. Die Operatoren der Gruppen

$$G_\alpha = \{s_2, s_3, \ldots, s_\alpha\} \qquad (\alpha = 2, 3, 4, \ldots, \nu)$$

sind untereinander bis auf Operatoren von $G_{\alpha-1}$ vertauschbar; II. die niedrigste Potenz von s_α, die in $G_{\alpha-1}$ vorkommt, hat eine Primzahl zum Exponenten. Dieser Satz stammt von Galois. Kürzer können wir ihn so aussprechen: Eine Gruppe G ist

auflösbar, wenn sie einen auflösbaren Teiler H selbstkonjugiert enthält, derart, daß der Index von G zu H eine Primzahl ist (Frobenius).

§ 88. Eine andere charakteristische Eigenschaft auflösbarer Gruppen hat C. Jordan angegeben; sie knüpft an die Konstitution der Hauptreihe an.

Wir wissen (§ 57, S. 74), daß wenn sich zwischen zwei aufeinanderfolgende Glieder der Hauptreihe noch Glieder der Kompositionsreihe einschieben lassen, diese auf gleiche Zahlfaktoren der Zusammensetzung führen. In unserem Falle auflösbarer Gruppen stößt man also dabei auf dieselbe Primzahl p.

Nun mögen in den Kompositionsreihen, die von H zu J führen, unmittelbar vor J die Gruppen H_1, H_2, H_3, ... möglich sein; dann ist

$$(1) \qquad H = \{\mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \ldots\}.$$

Da ferner der Index von J zu einem jeden H_α gleich der Primzahl p ist, so gibt es nach dem in § 57 Besprochenen Operatoren $\tau_1, \tau_2, \tau_3, \ldots$ der Art, daß

$$\mathsf{H}_1 = \{J, \tau_1\}, \quad \mathsf{H}_2 = \{J, \tau_2\}, \quad \mathsf{H}_3 = \{J, \tau_3\}, \quad \ldots,$$

und daß die niedrigste Potenz von $\tau_1, \tau_2, \tau_3, \ldots$, die in J vorkommt, jedesmal die $p$te ist. Dabei wird

$$(2) \qquad \left\{\begin{array}{r|r|r|l} \mathsf{H}_1 = \tau_1^\alpha J & \mathsf{H}_2 = \tau_2^\alpha J & \mathsf{H}_3 = \tau_3^\alpha J & \ldots \\ = J\tau_1^\alpha & = J\tau_2^\alpha & = J\tau_3^\alpha & \ldots \\ \multicolumn{4}{c}{(\alpha = 0, 1, 2, \ldots, p-1).} \end{array}\right.$$

Weiter folgt aus der Definition der Kompositionsreihe

$$\tau_1^{-1} J \tau_1 = J, \quad \tau_2^{-1} J \tau_2 = J, \quad \tau_3^{-1} J \tau_3 = J, \quad \ldots$$

Da in den Kompositionsreihen die Gruppe $\{\mathsf{H}_1, \mathsf{H}_2\}$ den Gruppen H_1 sowie H_2 unmittelbar voraufgeht, so ist

$$\tau_2^{-1}\tau_1\tau_2 = \tau_1^\delta i_1, \quad \tau_1^{-1}\tau_2^{-1}\tau_1 = i_2\tau_2^\varepsilon,$$

wenn i_1, i_2 Operatoren von J bedeuten. Daraus folgt, daß

$$\tau_1^{-1}\tau_2^{-1}\tau_1\tau_2 = \tau_1^{\delta-1} i_1 = i_2 \tau_2^{-\varepsilon+1}$$

ein zu H_1 wie zu H_2 gehöriger Operator ist, und da $\}\mathsf{H}_1, \mathsf{H}_2\{ = J$, so muß $\delta = 1$ und $\varepsilon = -1$ werden, d. h.

$$(3) \qquad \tau_1\tau_2 = \tau_2\tau_1 i', \quad \tau_\alpha\tau_\beta = \tau_\beta\tau_\alpha i''.$$

Daraus kann man entnehmen, daß die Operatoren der Gruppe

$$H = \{J;\ \tau_1, \tau_2, \tau_3, \ldots\}$$

untereinander bis auf Operatoren von J vertauschbar sind. Denn man hat unter Benutzung von (2) und (3) z. B.

$$(\tau_1^\alpha\, i\, \tau_2^\beta\, i'\, \tau_3^\gamma\, i'')\,(\tau_1^\delta\, i'''\, \tau_2^\varepsilon\, i^{IV}\, \tau_3^\zeta\, i^V)$$

$$= (\tau_1^\alpha\, \tau_2^\beta\, \tau_3^\gamma\, i_0)\,(\tau_1^\delta\, \tau_2^\varepsilon\, \tau_3^\zeta\, i_0') = (\tau_1^\delta\, \tau_2^\varepsilon\, \tau_3^\zeta\, i_0')\,(\tau_1^\alpha\, \tau_2^\beta\, \tau_3^\gamma\, i_0) \cdot i''\,.$$

Wenn umgekehrt die Operatoren von H bis auf die von J miteinander vertauschbar sind, dann ist der Index von J zu H_α eine Primzahl. Um dies klarzulegen, denken wir uns den Index von J zu H_α in seine Primfaktoren $q \cdot q' \cdot q'' \ldots$ zerlegt und nehmen an, es gebe mehrere gleiche oder ungleiche q; aus dieser Annahme wollen wir einen Widerspruch herleiten.

Da J ein selbstkonjugierter Teiler von H_α ist, so besteht eine Faktorgruppe $\Gamma = \mathsf{H}_\alpha / J$ der Ordnung $q \cdot q' \cdot q'' \ldots$ und, wie der Cauchysche Satz zeigt, in dieser Faktorgruppe Γ ein Teiler der Ordnung q. Nach § 30, S. 45 entspricht diesem echten Teiler der Gruppe Γ ein echter Teiler von H_α, der J als echten Teiler enthält; dieser heiße $\varDelta$. Wegen der Vertauschbarkeit der Operatoren von H untereinander bis auf Operatoren von J ist $\bar{\mathsf{H}}_\alpha^{-1}\, \varDelta\, \bar{\mathsf{H}}_\alpha = \varDelta$, also $\varDelta$ ein selbstkonjugierter Teiler von H_α, der $< \mathsf{H}_\alpha$ und $> J$ ist. Das kann nicht sein, da J ein selbstkonjugierter Maximalteiler von H_α war.

Faßt man die Resultate dieses Paragraphen zusammen, so erkennt man: Die Gruppe G ist dann und nur dann auflösbar, wenn in ihrer Hauptreihe

$$G,\ H,\ J,\ K,\ \ldots,\ M,\ 1$$

die Operatoren jedes Gliedes bis auf Operatoren des nächstfolgenden miteinander vertauschbar sind.

§ 89. Aus § 54, S. 71 entnehmen wir, daß wenn eine Gruppe G auflösbar ist, auch jeder ihrer Teiler H eine auflösbare Gruppe wird. Denn alle Zahlfaktoren der Komposition von H sind Teiler derer von G, und da die von G Primzahlen sind, so sind es auch die von H.

Ist die auflösbare Gruppe G (einstufig oder mehrstufig) isomorph zu der Gruppe Γ, so ist auch Γ auflösbar. In der Tat, wenn K und L zwei aufeinanderfolgende Glieder der Kompositionsreihe von G sind, so wird ihr Index eine Primzahl werden, etwa p. Sind nun K und Λ die Teiler aus Γ, die den Teilern K und L aus G entsprechen, so ist wegen

$$\overline{K}^{-1} L \overline{K} = L \quad \text{auch} \quad \overline{\mathsf{K}}^{-1} \Lambda \overline{\mathsf{K}} = \Lambda$$

und der Index von Λ zu K ist gleich dem von L zu K, also auch gleich der Primzahl p. Dadurch ist der Beweis geliefert.

Ist die Gruppe G mehrstufig isomorph zu der auflösbaren Gruppe Γ; entspricht ferner der Einheit in Γ eine auflösbare Gruppe M in G, so ist auch G auflösbar. Man kann nämlich eine Kompositionsreihe von G so herstellen, daß sie als ein Glied den in G selbstkonjugierten Teiler M enthält. An ihr erkennt man dann sofort die Richtigkeit des behaupteten Satzes.

§ 90. Aus unseren früheren Untersuchungen können wir die nachstehenden Sätze entnehmen.

Die alternierende Substitutionengruppe und folglich auch die symmetrische sind nicht auflösbar, wenn ihr Grad größer als 4 ist; die abstrakten, ihnen isomorphen Gruppen sind ebensowenig auflösbar (§ 64, S. 81).

Jede Abelsche Gruppe ist auflösbar (§ 65, S. 83), insbesondere jede zyklische Gruppe.

Jede Gruppe von Primzahlpotenzordnung ist auflösbar (§ 59, S. 76).

Durch Zusammenstellung des letzten Satzes mit dem zweiten des vorigen Paragraphen gelangt man zu einem weiteren Kriterium für auflösbare Gruppen. Zu seiner Herleitung betrachten wir ein Glied der Hauptreihe H, die zur auflösbaren Gruppe G gehört; dann muß die Faktorgruppe G/H auflösbar sein, und H ist es natürlich ebenfalls. Umgekehrt ist aber die Auflösbarkeit von G/H nebst der von H auch hinreichend für die von G. So sieht man:

Für auflösbare Gruppen G ist es charakteristisch, daß entweder ihre Ordnung die Potenz

einer Primzahl ist, oder daß sie eine von der Einheit verschiedene, selbstkonjugierte Untergruppe H von Primzahlpotenzordnung enthalten, für die die Faktorgruppe G/H auflösbar ist. Dabei ist H als die letzte in der Hauptreihe von G vor der Einheit stehende Gruppe zu denken. Der Unterschied zwischen unserem ersten, Galoisschen (§ 87, S. 116), und dem jetzt hergeleiteten, von Frobenius angegebenen Kriterium besteht hauptsächlich darin, daß der betrachtete selbstkonjugierte Teiler H von G beim ersten eine möglichst hohe, beim zweiten eine möglichst niedrige Ordnung besitzt.

§ 91. Aus seinen im vorigen Kapitel besprochenen Resultaten hat Sylow den folgenden Satz über die Auflösbarkeit gewisser Gruppen hergeleitet.

Ist die Ordnung r einer Gruppe G durch

$$r = p_1^\alpha p_2^\beta p_3^\gamma p_4^\delta \cdots$$

bestimmt, wobei die $p_1, p_2, p_3, p_4, \ldots$ Primzahlen bedeuten, die den Ungleichungen

$$p_1 > p_2^\beta p_3^\gamma p_4^\delta \cdots; \quad p_2 > p_3^\gamma p_4^\delta \cdots; \quad p_3 > p_4^\delta \cdots; \quad \cdots$$

genügen, dann ist G auflösbar.

G enthält nach § 79, S. 101 eine Gruppe H der Ordnung p_1^α als Teiler. Dabei wird (§ 81, S. 104)

$$r = p_1^\alpha m(1 + p_1 k),$$

wobei $p_1^\alpha m$ die Ordnung der Zwischengruppe von H in G bedeutet, während $(1 + p_1 k)$ die Anzahl aller Teiler von G angibt, die die Ordnung p_1^α haben. Hier ist nun

$$p_2^\beta p_3^\gamma p_4^\delta \cdots = m(1 + p_1 k) < p_1;$$

demnach muß $k = 0$ sein, d. h. G enthält nur eine einzige Gruppe der Ordnung p_1^α als Teiler, nämlich H. Folglich ist H selbstkonjugiert in G; denn jede Transformierte $G^{-1} H G$ muß wieder gleich H werden. Wir setzen $G/H = \Gamma$; der letzte Satz des vorigen Paragraphen zeigt, daß, wenn Γ und H auflösbar sind, auch G auflösbar ist. Für H folgt diese Eigenschaft aus dem letzten Satze über Gruppen von Primzahlpotenzordnung. Für Γ ist es der gleiche Satz wie der behauptete unter der vereinfachenden Voraus-

setzung einer geringeren Anzahl von Primfaktoren für die Ordnung der Gruppe. Da für $r = p_1^\alpha$ und für $r = p_1^\alpha p_2^\beta$ die Behauptung begründet ist, so folgt der allgemeine Satz durch strenge Induktion.

§ 92. Frobenius hat durch ähnliche Schlüsse aus seinem Theoreme (§ 84, S. 110) einen wichtigen Satz hergeleitet, der gewissermaßen den entgegengesetzten Pol zu dem Theorem über die Auflösbarkeit der Gruppen von Primzahlpotenzordnung bildet.

Sind $p_1 < p_2 < \cdots < p_n$ n verschiedene Primzahlen, so ist jede Gruppe G von der Ordnung $r = p_1 p_2 \ldots p_n$ auflösbar. Es ist also charakteristisch, daß die Ordnung von G durch kein Quadrat teilbar ist.

Nach dem erwähnten Theorem gibt es in G genau $p_{\lambda+1} \cdot p_{\lambda+2} \cdot \ldots \cdot p_n$ Operatoren, deren Ordnung in dem Produkte $p_{\lambda+1} \cdot p_{\lambda+2} \cdot \ldots \cdot p_n$ aufgeht,

$$(\lambda = n - 1, n - 2, n - 3, \ldots);$$

zunächst also genau p_n Operatoren, deren Ordnung in p_n aufgeht. Sie bilden eine Gruppe, da sie die Potenzen eines jeden unter ihnen sind, der von der Einheit verschieden ist. Diese Gruppe heiße G_{n-1}. Da es nur eine solche Gruppe in G gibt, so ist G_{n-1} ein selbstkonjugierter Teiler von G. Die Auflösbarkeit von G wird durch die von G_{n-1} und von G/G_{n-1} bedingt (§ 89). Für G_{n-1} steht sie fest, da die Ordnung von G_{n-1} eine Primzahl ist; für G/G_{n-1} wird sie durch den zu beweisenden Satz geliefert, falls er unter der vereinfachenden Voraussetzung einer geringeren Anzahl von Faktoren für die Ordnung der Gruppe bewiesen ist. Somit erkennt man auch hier die Richtigkeit des Theorems durch strenge Induktion, da es für $n = 2$ klar ist.

Man sieht, daß G/G_{n-1} die Ordnung $p_1 p_2 \ldots p_{n-1}$ besitzt. Wendet man auf diese Faktorgruppe den Hilfssatz § 84 an, so folgt, daß G/G_{n-1} einen und nur einen Teiler der Ordnung p_{n-2} selbstkonjugiert enthält. Diesem Teiler entspricht in G wegen der isomorphen Beziehungen ein Teiler der Ordnung $p_{n-1} \cdot p_n$, der G_{n-1} selbstkonjugiert enthält; er mag G_{n-2} heißen; G_{n-2} besteht aus allen Operatoren von G, deren Ordnung in $p_{n-1} \cdot p_n$ aufgeht. G/G_{n-2} hat die Ordnung $p_1 p_2 \ldots p_{n-2}$ usw.

§ 93. An das erhaltene Resultat hat Frobenius folgende Schlüsse angeknüpft: Es seien a und b zwei beliebige Operatoren der im vorigen Paragraphen betrachteten Gruppe G, und α bzw. β ihre Ordnungen. Ist $p_{\lambda+1}$ die kleinste in $\alpha \cdot \beta$ enthaltene Primzahl, so gehen nach den über G gemachten Voraussetzungen α und β beide in $p_{\lambda+1} \cdot p_{\lambda+2} \cdot \ldots \cdot p_n$ auf. Daher gehören beide der Gruppe G_λ an, und mithin auch ihr Produkt. Folglich ist auch die Ordnung von $a \cdot b$ ein Divisor von $p_{\lambda+1} p_{\lambda+2} \ldots p_n$, d. h.: Die Ordnung des Produktes mehrerer Operatoren von G ist durch keine Primzahl teilbar, die kleiner ist als die kleinste Primzahl, die in die Ordnung eines der Faktoren aufgeht.

§ 94. Mittels der gleichen Prinzipien, wie sie in § 92 angewendet wurden, läßt sich auch der folgende erweiternde Satz beweisen (Frobenius).

Sind $p_1 < p_2 < \ldots < p_n < p$ $(n+1)$ verschiedene Primzahlen, so ist jede Gruppe G der Ordnung

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n \cdot p^\alpha,$$

wo α eine beliebige positive ganze Zahl bedeutet, auflösbar.

Nach dem Sylowschen Satze nämlich enthält G eine Untergruppe G_n der Ordnung p^α und nur eine, weil nach dem Frobeniusschen Satze (§ 84, S. 110) in G genau p^α Operatoren vorkommen, deren Ordnung in p^α aufgeht. Folglich ist G_n ein selbstkonjugierter Teiler von G, und $\Gamma = G/G_n$ eine zu G isomorphe Gruppe der Ordnung $p_1 p_2 \ldots p_n$. Demnach ist G auflösbar (§ 92, S. 121); denn Γ und G_n sind es.

§ 95. Von weiteren Resultaten, die durch die Untersuchungen von Burnside und vor allem von Frobenius zutage gefördert sind, führen wir, ohne auf die Beweise näher einzugehen, die folgenden an.

Sind p und q zwei verschiedene Primzahlen, so ist jede Gruppe der Ordnung $p^\alpha q$ auflösbar.

Sind p und q zwei verschiedene Primzahlen, und ist q^β die niedrigste Potenz von q, die $\equiv 1 \pmod p$ wird, so ist jede Gruppe der Ordnung $p^\alpha q^\beta$ auflösbar.

Sind $p_1 < p_2 < \ldots < p_n < q < r$ verschiedene Prim-

zahlen, so ist eine Gruppe der Ordnung $p_1 p_2 \ldots p_n q^2 r^\gamma$ im allgemeinen auflösbar.

Sind $p < q < r$ drei verschiedene Primzahlen, so ist eine jede Gruppe der Ordnung $p^2 q r^\gamma$ auflösbar.

Sind p_1, p_2 zwei Primzahlen und $p_1 < p_2$, so sind die Gruppen, deren Ordnung von einer der Formen $p_1 p_2^\alpha$, $p_1^2 p_2^\alpha$, $p_1^3 p_2^\alpha$, $p_1^4 p_2^\alpha$, $p_1^5 p_2^\alpha$, $p_1^\alpha p_2$, $p_1^\alpha p_2^2$ ist, auflösbar.

Sind p und q zwei verschiedene Primzahlen, so ist jede Gruppe der Ordnung $p^\alpha q^\beta$, in der die Teiler der Ordnung p^α und q^β Abelsche Gruppen sind, auflösbar.

Sind $p, q, \ldots, r, s$ verschiedene Primzahlen, so ist jede Gruppe der Ordnung $p^\alpha q^\beta \ldots r^\gamma s^\delta$, in der die Teiler der Ordnung $p^\alpha, q^\beta, \ldots, r^\gamma$ zyklische Gruppen sind, auflösbar.

Jede Gruppe, deren Ordnung kleiner als 60 ist, ist auflösbar.

Ferner sei auf spätere Untersuchungen über auflösbare Gruppen in den §§ 118, 134 hingewiesen.

---

9. Kapitel.

Substitutionengruppen. — Transitivität.

§ 96. Wir haben früher gesehen, daß jede abstrakte Gruppe sich als Substitutionengruppe darstellen läßt, und zwar zunächst als reguläre, d. h. als solche, bei der die Ordnung gleich dem Grade ist (§ 18, S. 28). Von dieser regulären Gruppe kann man dann zu jeder einstufig isomorphen übergehen. Umgekehrt läßt sich jede Substitutionengruppe als abstrakte Gruppe von gleicher Ordnung und Konstitution darstellen. Hieraus geht hervor, daß die wesentlichen Eigenschaften der Gruppen in beiden Darstellungsarten zutage treten werden.

Es gibt aber auch Eigenschaften, die an der Darstellung durch Substitutionen haften und bei den abstrakten Gruppen kein Analogon aufweisen. Mit solchen Eigenschaften wollen wir uns hier beschäftigen. Zu ihnen gehört in erster Linie die Transitivität.

Wir nehmen an, es sei eine Substitutionengruppe G der Ordnung r und des Grades n vorgelegt. Die n Elemente der Gruppe seien

(1) $$a_1\,,\ a_2\,,\ a_3\,,\ \ldots,\ a_{n-1}\,,\ a_n\,,$$

und die aus ihnen gebildeten Substitutionen von G

(2) $$s_1\,,\ s_2\,,\ s_3\,,\ \ldots,\ s_{r-1}\,,\ s_r \qquad (s_1 = 1)\,.$$

Wir denken die Substitutionen in Zykeldarstellung geschrieben. Dann ist es möglich, daß, wenn a_1 ein beliebiges Element aus (1) bedeutet, in den Zykeln aller s_α von (2) die n Folgen

(3) $$a_1 a_1\,,\ a_1 a_2\,,\ a_1 a_3\,,\ \ldots,\ a_1 a_{n-1}\,,\ a_1 a_n$$

vorkommen. In diesem Falle heißt G eine transitive Substitutionengruppe. Kommen nicht alle Folgen (3) vor, so heißt G intransitiv. So ist die Gruppe

$$1\,,\ (a_1 a_2 a_3 a_4)\,,\ (a_1 a_3)(a_2 a_4)\,,\ (a_1 a_4)(a_2 a_3)$$

transitiv; dagegen die Gruppe

$$1\,,\ (a_1 a_3)(a_2 a_4)$$

intransitiv.

Man unterscheidet einfache und mehrfache Transitivität bei Substitutionengruppen. Eine Gruppe heißt k-fach transitiv, falls sie durch ihre Substitutionen (2) k feste Elemente, etwa $a_1, a_2, a_3, \ldots, a_k$, in k beliebige $a_{i_1}, a_{i_2}, a_{i_3}, \ldots, a_{i_k}$ überführt, falls also eine Substitution von (2) die Folgen

(4) $$a_1 a_{i_1}\,,\ a_2 a_{i_2}\,,\ a_3 a_{i_3}\,,\ \ldots,\ a_n a_{i_n}$$

bei willkürlichen $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$ aufweist. Die oben definierte Transitivität ist also einfache Transitivität; sie bezieht sich auf den besonderen Fall $k = 1$.

Eine k-fach transitive Gruppe ist auch $(k-1)$-fach, $(k-2)$-fach, ..., einfach transitiv.

Eine k-fach transitive Gruppe gibt transformiert wiederum eine solche.

Eine k-fach transitive Gruppe enthält eine Substitution aus (2), die k beliebige Elemente in k beliebige umwandelt, also etwa

(5) $$a_{i_1} \text{ in } a_{h_1}\,,\quad a_{i_2} \text{ in } a_{h_2}\,,\quad \ldots,\quad a_{i_k} \text{ in } a_{h_k}\,.$$

Denn nach der Definition gibt es zwei Substitutionen in (2)

s_i mit den Folgen $a_1 a_{i_1}$, $a_2 a_{i_2}$, $a_3 a_{i_3}$, ..., $a_k a_{i_k}$;

s_h mit den Folgen $a_1 a_{h_1}$, $a_2 a_{h_2}$, $a_3 a_{h_3}$, ..., $a_k a_{h_k}$;

dann liefert das Produkt $s_i^{-1} s_h$ die geforderten Folgen (5).

§ 97. Gegeben sei eine k-fach transitive Gruppe G der Elemente (1). Der Teiler von G, der die Elemente $a_1, a_2, \ldots, a_k$ nicht umsetzt, heiße G_1. Zu G_1 gehört die Substitution $s_1 = 1$. Nun sei s_i eine Substitution von G mit den Folgen $a_1 a_{i_1}, \ldots, a_k a_{i_k}$; dann haben alle Substitutionen des Komplexes $G_1 s_i$ die gleichen Folgen $a_1 a_{i_1}$, ..., $a_k a_{i_k}$; und umgekehrt: ist σ eine Substitution von G mit diesen Folgen, so gehört das Produkt $\sigma \cdot s_i^{-1}$ zu G_1, und es ist $\sigma = G_1 s_i$. Man kann daher G in den Summanden G_1 und seine Nebenkomplexe zerlegen

$$G = G_1 + G_1 s_2 + G_1 s_3 + \ldots + G_1 s_\tau, \tag{6}$$

so daß alle Substitutionen jedes Summanden der rechten Seite die Elemente $a_1, a_2, \ldots, a_k$ in dieselben Elemente umwandeln; und die zweier verschiedenen Summanden in verschiedene Elemente. Die Zahl τ ist leicht zu bestimmen; sie gibt an, wie viele Variationen ohne Wiederholung aus n Elementen zur $k$ten Klasse gebildet werden können; dies liefert nämlich die Anzahl der möglichen Folgen für die k Elemente $a_1, a_2, \ldots, a_{k-1}, a_k$, die bei den n Elementen (1) auftreten. Es ist daher

$$\tau = n(n-1)(n-2)\ldots(n-k+1).$$

Die Anzahl der Substitutionen auf der rechten Seite von (6) ist also das τ-fache der Ordnung von G_1. Man hat daher: Die Ordnung einer k-fach transitiven Gruppe des Grades n ist gleich dem Produkte aus

$$n(n-1)(n-2)\ldots(n-k+1)$$

in die Ordnung des Teilers der Gruppe, der k willkürliche Elemente der Gruppe ungeändert läßt. Insbesondere ist die Ordnung einer einfach transitiven Gruppe gleich dem Produkte aus ihrem Grade in die Ordnung des Teilers, der eins ihrer Elemente an seiner Stelle läßt.

§ 98. Die Richtigkeit des folgenden Satzes ist leicht einzusehen: Ist G eine k-fach transitive Gruppe und H ein Teiler von G, der $\alpha (< k)$ Elemente ungeändert läßt, so ist H noch $(k - \alpha)$-fach transitiv.

Wir wollen eine Umkehrung dieses Satzes beweisen. Es sei die Gruppe G transitiv und der Teiler H von G, der ein Element ungeändert läßt, genau k-fach transitiv, dann ist G $(k + 1)$-fach transitiv.

G möge die Elemente $x_0, x_1, x_2, \ldots, x_n$ haben, H das Element x_0 ungeändert lassen. Um eine Substitution mit den $(k + 1)$ geforderten Folgen

(7) $$x_0 x_0'; \; x_1 x_1'; \; \ldots; \; x_k x_k'$$

herzustellen, wo $x_0', x_1', \ldots, x_k'$ zu den Elementen von G gehören, verfährt man so: Man wählt aus G eine Substitution s mit der Folge $x_0 x_0'$; dies s möge die weiteren Folgen

$$x_1 x_1'', \; x_2 x_2'', \; \ldots, \; x_k x_k''$$

haben, wo die x_α'' zu den Elementen von G gehören. Dann bildet man die gleichfalls k-fach transitive Gruppe $s^{-1} H s$, die nun x_0' ungeändert läßt. Aus ihr wählt man eine Substitution t mit den k Folgen

$$x_1'' x_1', \; x_2'' x_2', \; \ldots, \; x_k'' x_k',$$

so erfüllt das Produkt $s \cdot t$ die $(k + 1)$ Forderungen aus (7).

Ebenso beweist man: Ist die Gruppe G von α-facher Transitivität und der Teiler H von G, der α Elemente ungeändert läßt, k-fach transitiv, so ist G $(k + \alpha)$-fach transitiv.

Man überzeugt sich leicht, daß der Nachweis auf den gleichen Schlüssen wie der des eben bewiesenen Theorems beruht. Der Satz selbst ist die Umkehrung des zu Anfang dieses Paragraphen gegebenen.

Hieraus kann man weiter schließen:

Die alternierende Gruppe von n Elementen ist $(n - 2)$-fach transitiv.

Wir nehmen im voraufgehenden Satze für G die alternierende Gruppe aus n Elementen und setzen $\alpha = 1$. Der Teiler von G, der eins der n Elemente nicht umsetzt, sei H. Dann ist H die alternierende Gruppe der übrigen $(n - 1)$ Elemente, wie man sofort sieht. Gesetzt nun,

H wäre $(n-3)$-fach transitiv, dann zeigt der vorangehende Satz, daß G sogar $(n-2)$-fach transitiv ist. Nun ist das Theorem für $n = 3$ richtig, also gilt es allgemein.

§ 99. Enthält eine $k(>1)$-fach transitive Gruppe eine Zirkularsubstitution von drei Elementen, so enthält sie die alternierende Gruppe. Es sei $\sigma = (x_1 x_2 x_3)$ die Zirkularsubstitution von drei Elementen in G. Da die Gruppe G mindestens zweifach transitiv ist, so enthält sie eine Substitution t mit den Folgen $x_3 x_3$ und $x_1 x_4$; t möge auf x_2 folgen lassen x_λ. Wir setzen $t^{-1}\sigma t = (x_3 x_4 x_\lambda) = \tau$. Je nachdem dieses $x_\lambda = x_1$ oder $= x_2$ oder gleich einem neuen Elemente x_5 ist, wird

$$\tau\sigma^2\tau^{-1} \quad \text{oder} \quad \tau\sigma^2\tau^{-1} \quad \text{oder} \quad \tau^{-1}\sigma\tau$$

gleich $(x_1 x_2 x_4)$; und ebenso kann man die Existenz der Zirkularsubstitutionen

$$(x_1 x_2 x_5)\,,\ (x_1 x_2 x_6)\,,\ \ldots,\ (x_1 x_2 x_n)$$

nachweisen. Da ferner

$$(x_1 x_2 x_b)(x_1 x_2 x_a)(x_1 x_2 x_b)^{-1} = (x_1 x_a x_b)\,,$$

$$(x_1 x_2 x_c)(x_1 x_2 x_b)(x_1 x_2 x_a)(x_1 x_2 x_b)^{-1}(x_1 x_2 x_c)^{-1} = (x_a x_b x_c)$$

ist, so enthält nach § 11, S. 14 die Gruppe G die alternierende.

Noch einfacher ist der Beweis des folgenden Satzes: Enthält eine $k(>1)$-fach transitive Gruppe eine Transposition, so ist sie symmetrisch. Es sei $\sigma = (x_1 x_2)$ diese Transposition. Da die Gruppe mindestens zweifach transitiv ist, so gibt es eine Substitution t, die x_1 ungeändert läßt und x_2 in x_3 überführt. Man hat dann

$$t^{-1}\sigma t = (x_1 x_3)$$

und kann ebenso die Existenz von

$$(x_1 x_4)\,,\ (x_1 x_5)\,,\ \ldots,\ (x_1 x_n)$$

nachweisen. Nach § 11, S. 14 ist die Gruppe die symmetrische.

§ 100. Zu einer Erweiterung dieser Sätze gelangen wir durch Betrachtung einer k-fach transitiven Gruppe $(k > 2)$, deren von der Einheit verschiedene Substitutionen mindestens q Elemente umsetzen und die auch wirklich Substitutionen

mit genau q Elementen besitzen. Die Substitutionengruppe heißt dann eine Gruppe der $q$ten Klasse.

Wir nehmen zuerst $q > k$ an. Es sei

$$s = (x_1 x_2 \ldots) \ldots (\ldots x_{k-1} x_k \ldots) \ldots (\ldots x_q)$$

eine der Substitutionen, die möglichst wenig, also q Elemente umstellen. Wegen der k-fachen Transitivität gibt es eine Substitution aus G

$$t = (x_1)(x_2) \ldots (x_{k-1})(x_k x_l \ldots) \ldots,$$

in der x_l ein schon in s vorkommendes, von $x_1, x_2, \ldots, x_k$ verschiedenes Element bedeuten soll. Die Substitution t ist dabei, wie man sieht, von der Einheit verschieden.

Man hat dann

$$t^{-1} s t = (x_1 x_2 \ldots) \ldots (\ldots x_{k-1} x_l \ldots) \ldots (\ldots x_0),$$

und hierin können höchstens $(q - k)$ neue, d. h. nicht schon in s enthaltene Elemente x auftreten. In dem Produkte $(t^{-1} s t) s^{-1}$ fallen mindestens die $(k - 2)$ ersten Elemente $x_1, x_2, \ldots, x_{k-2}$ weg; das Produkt enthält also höchstens

$$q + (q - k) - (k - 2) = 2q - 2k + 2$$

Elemente. Diese Zahl muß $\geqq q$ sein. Also wird

$$q \geqq 2k - 2.$$

Ist daher $q < 2k - 2$, dann muß q sogar $< k$ sein, da aus $q > k$ nach dem Bewiesenen $q \geqq 2k - 2$ folgen würde.

Wir untersuchen zweitens den Fall $q \leqq k$. Wir gehen wieder von einem

$$s = (x_1 x_2 \ldots) \ldots (\ldots x_{q-1} x_q)$$

aus, das zu den Substitutionen geringster Elementenzahl gehört. Wegen der k-fachen Transitivität gibt es in G ein

$$t = (x_1)(x_2) \ldots (x_{q-1})(x_q x_{q+1}),$$

wo x_{q+1} ein neues, d. h. nicht schon in s enthaltenes Element bedeutet. Man hat dann ohne Änderung der ersten $(q - 1)$ Elemente gegen s

$$t^{-1} s t = (x_1 x_2 \ldots) \ldots (\ldots x_{q-1} x_{q+1}),$$

also

$$t^{-1} s t s^{-1} = (x_{q-1} x_{q+1} x_q).$$

Somit enthält die Substitutionengruppe eine Zirkularsubstitution von drei Elementen, umschließt also nach dem vorigen Paragraphen die alternierende Gruppe.

Hat eine $k(>2)$-fach transitive Gruppe Substitutionen von weniger als $(2k-2)$ Elementen, die von der Einheit verschieden sind, so ist sie alternierend oder symmetrisch.

Es sei nun n der Grad einer k-fach $(k>2)$ transitiven Substitutionengruppe, die die alternierende Gruppe der n Elemente nicht enthält. Infolge der Transitivität enthält die Gruppe Substitutionen, die $(k-1)$ Elemente nicht ändern und außerdem eine beliebige Folge $x_k x_l$ mit $l \neq k$ enthalten, also nicht $=1$ sind. Nach dem eben bewiesenen Satze ist dann $n-(k-1)=n-k+1 \geqq 2k-2$ und $k \leqq \frac{1}{3}n+1$; d. h.:

Eine Gruppe vom Grade n, die die alternierende Gruppe nicht enthält, kann nicht mehr als $(\frac{1}{3}n+1)$-fach transitiv sein.

Weitere Untersuchungen nach dieser Richtung haben unter anderen zu den folgenden Resultaten geführt:

Enthält eine Substitutionengruppe vom Grade n die alternierende Gruppe ihrer Elemente nicht, so versetzt jede ihrer Substitutionen bei mehr als einfacher Transitivität mehr als $(\frac{1}{4}n-1)$ Elemente; bei mehr als zweifacher Transitivität mehr als $(\frac{1}{3}n-1)$ Elemente; und bei mehr als dreifacher Transitivität nicht weniger als $(\frac{1}{2}n-1)$ Elemente (Bochert).

§ 101. Wir betrachten jetzt eine einfach transitive Gruppe G des Grades n und der Ordnung $r=n\nu$ mit den Elementen $x_1, x_2, \ldots, x_n$. Dabei bedeutet ν die Ordnung eines der Teiler von G, der ein beliebiges Element x_α von G ungeändert läßt (§ 97). Wir bezeichnen mit $G_1, G_2, \ldots, G_n$ die Teiler von G, die bzw. das Element $x_1, x_2, \ldots, x_n$ nicht umstellen. Hat s die Folge $x_1 x_\lambda$, so ist

$$s_\lambda^{-1} G_1 s_\lambda = G_\lambda ;$$

also sind alle G_λ konjugiert und einander ähnlich, und jedes G_α enthält ebenso viele Substitutionen, die genau $\varrho = 1, 2, \ldots, n-1$ Elemente umsetzen, wie jedes andere G_ϱ. Wir wollen die Anzahl der Substitutionen

von G_1, die genau ϱ Elemente umsetzen, mit ν_ϱ bezeichnen. Dann ist, da ν die Ordnung von G_1 angibt,

$$(8)\qquad \nu = \nu_{n-1} + \nu_{n-2} + \cdots + \nu_2 + \nu_0 \qquad (\nu_0 = 1)\,.$$

In G_1 gibt es ν_ϱ Substitutionen, die genau ϱ Elemente umstellen; in $G_1, G_2, \ldots, G_n$ zusammen $n \cdot \nu_\varrho$. Diese sind aber nicht alle voneinander verschieden; jede der Substitutionen tritt $(n-\varrho)$-mal auf. In G gibt es also nur $\frac{n}{n-\varrho} \cdot \nu_\varrho$ solcher Substitutionen. Folglich ist die Anzahl aller Substitutionen in G, die weniger als alle n Elemente umstellen,

$$\frac{n}{1}\nu_{n-1} + \frac{n}{2}\nu_{n-2} + \cdots + \frac{n}{n-\varrho}\nu_\varrho + \cdots + \frac{n}{n}\nu_0\,.$$

Da die Anzahl aller Substitutionen von G wegen (8) gleich

$$r = n\nu = n\nu_{n-1} + n\nu_{n-2} + \cdots + n\nu_\varrho + \cdots + n \cdot \nu_0$$

ist, so stellen genau

$$(8\text{a})\left\{\begin{aligned} r - \Big[\frac{n}{1}\nu_{n-1} + \frac{n}{2}\nu_{n-2} + \cdots + \frac{n}{n-\varrho}\nu_\varrho + \cdots + \frac{n}{n}\nu_0\Big] \\ = n\Big[\frac{1}{2}\nu_{n-2} + \frac{2}{3}\nu_{n-3} + \cdots + \frac{n-\varrho-1}{n-\varrho}\nu_\varrho + \cdots + \frac{n-1}{n}\nu_0\Big] \end{aligned}\right.$$

Substitutionen alle Elemente um. Keins der ν_ϱ ist negativ und $\nu_0 = 1$. Also enthält jede einfach transitive Gruppe mindestens $(n-1)$ Substitutionen, die alle Elemente umsetzen. Enthält sie mehr als $(n-1)$, dann hat sie auch Substitutionen, die weniger als $(n-1)$ Elemente umsetzen.

§ 102. Gegeben sei die Gesamtheit der Substitutionen $\sigma_1, \sigma_2, \sigma_3, \ldots$ einer einfach transitiven Gruppe G, die alle Elemente umsetzen. Wir bilden den Teiler

$$H = \{\sigma_1, \sigma_2, \sigma_3, \ldots\}$$

von G und behaupten, H sei transitiv. Zunächst ist klar, daß H selbstkonjugiert in G ist; denn jede Transformation führt die Gesamtheit der σ in sich selbst über. Nun nehmen wir H als intransitiv an; dabei sollen

$$(9)\qquad a_1, a_2, \ldots;\quad b_1, b_2, \ldots;\quad c_1, c_2, \ldots;\quad d_1, d_2, \ldots$$

die Elemente von G sein, derart bezeichnet, daß H die einzelnen $a_1, a_2, \ldots$ miteinander transitiv verbindet, ebenso die einzelnen $b_1, b_2, \ldots$ usf.; daß aber die a_λ mit den b_λ nicht durch H verbunden werden, usw. Transformiert man die Komplexe (9) durch die Substitutionen von G, so gehen alle a_λ in sich selbst über, oder alle a_λ in alle b_λ, oder in alle $c_\lambda \ldots$, weil im entgegengesetzten Falle noch eine weitere Verbindung der Elemente bestände, umfassender, als (9) sie anzeigt. Daraus folgt, daß die Anzahl der a_λ gleich der der b_λ, der $c_\lambda, \ldots$ ist; die einzelnen Komplexe (9) haben gleich viele Elemente. Wir bezeichnen diese Komplexe mit

(9a) $$A\,;\ B\,;\ C\,;\ D\,;\ \ldots\,;$$

dann stellt G die Komplexe $A, B, C, D, \ldots$ untereinander um. Jeder Substitution aus G entspricht eine Substitution der (9a) untereinander; diese Substitutionen bilden eine zu G isomorphe Gruppe Γ. Da G alle Elemente (9) transitiv verbindet, so ist auch Γ in den (9a) transitiv. Nach dem vorigen Paragraphen enthält Γ Substitutionen, die alle (9a) umstellen; eine von ihnen lasse etwa auf A folgen B. Ihr entspräche in G eine Substitution, die alle Elemente (9) umstellt, und die a_λ mit den b_λ verbindet. Das widerspricht der Annahme (9); folglich kann H nicht intransitiv sein.

Da $H = \{\sigma_1, \sigma_2, \sigma_3, \ldots\}$ transitiv ist, so gelten für diese Gruppe die Resultate aus § 101, S. 130. Es sei H_1 die Untergruppe von H, die a_1 nicht umsetzt; ν' sei ihre Ordnung; in H_1 gebe es ν'_ϱ Substitutionen, die genau ϱ Elemente umstellen. Aus $G > H$ folgt $\nu \geqq \nu'$, $\nu_\varrho \geqq \nu'_\varrho$. Da G und H dieselben Substitutionen haben, die alle Elemente umstellen, so ist nach (8a)

$$\frac{1}{2}\nu_{n-2} + \frac{2}{3}\nu_{n-3} + \ldots + \frac{n-\varrho-1}{n-\varrho}\nu_\varrho + \ldots + \frac{n-1}{n}\nu_0$$
$$= \frac{1}{2}\nu'_{n-2} + \frac{2}{3}\nu'_{n-3} + \ldots + \frac{n-\varrho-1}{n-\varrho}\nu'_\varrho + \ldots + \frac{n-1}{n}\nu'_0\,.$$

Daraus schließen wir wegen der eben aufgestellten Ungleichungen

$$\nu_{n-2} = \nu'_{n-2}\,,\quad \nu_{n-3} = \nu'_{n-3}\,,\quad \ldots,\quad \nu_1 = \nu'_1\,,\quad \nu_0 = \nu'_0\,;$$

d. h. H unterscheidet sich von G höchstens durch die Substitutionen, die nur ein Element ungeändert lassen. Allgemeiner: Stimmen zwei transitive Gruppen in den Substitutionen überein, die alle Elemente umsetzen, so unterscheiden sie sich höchstens in den Substitutionen voneinander, die genau ein Element nicht umsetzen.

§ 103. Wir wollen jetzt einen Typus von transitiven Gruppen genauer untersuchen, deren Grad gleich der Primzahl p ist. Nach § 97, S. 125 ist die Ordnung r jeder Gruppe G vom Grade p ein Vielfaches von p, und da G ein Teiler der symmetrischen Gruppe der p Elemente ist, so wird r ein Teiler von $p!$, ist also nur durch die erste Potenz von p teilbar. Der Cauchysche Satz zeigt, daß G einen Teiler H der Ordnung p enthält; der Sylowsche Zusatz, daß

$$r = p\,q(1 + \varkappa\,p) \tag{10}$$

ist, wo $p\,q$ die Ordnung der Zwischengruppe J von H in G angibt, und $(1 + \varkappa\,p)$ die Anzahl der sämtlichen in G vorhandenen Gruppen der Ordnung p; wir wissen, daß sie ein konjugiertes System bilden.

H besteht aus den Potenzen einer zyklischen Substitution. Wir bezeichnen ihre Elemente mit x_0, x_1, x_2, $\ldots$, x_{p-1} und setzen

$$H = \{s\} = \{(x_0\,x_1\,x_2\,\ldots\,x_{p-1})\}\,.$$

Die Zwischengruppe J von H besteht aus allen Substitutionen, die s in eine Potenz $s^\varkappa$ transformieren

$$s^\varkappa = (x_0\,x_\varkappa\,x_{2\varkappa}\,\ldots\,x_{(p-1)\varkappa}) = (x_\alpha\,x_{\alpha+\varkappa}\,x_{\alpha+2\varkappa}\,\ldots)\,.$$

Dabei sind die Indizes der x durch ihre kleinsten, nicht negativen Reste modulo p zu ersetzen. Nach § 32, S. 48 besteht der Inbegriff aller mit H vertauschbaren Substitutionen aus denen der Form

$$t_{\varkappa,\alpha} = \begin{pmatrix} x_0 & x_1 & x_2 & \ldots \\ x_\alpha & x_{\alpha+\varkappa} & x_{\alpha+2\varkappa} & \ldots \end{pmatrix} \qquad \begin{pmatrix} \alpha = 0, 1, 2, \ldots, p-1 \\ \varkappa = 1, 2, 3, \ldots, p-1 \end{pmatrix},$$

die wir einfacher nur durch Angabe der Indizesänderungen der x_z mit

$$t_{\varkappa,\alpha} = |z\,,\ \alpha + \varkappa\,z| \qquad \begin{pmatrix} \alpha = 0, 1, 2, \ldots, p-1 \\ \varkappa = 1, 2, 3, \ldots, p-1 \end{pmatrix}$$

bezeichnen. Hierbei kommen wir zu der analytischen Darstellung einer Gruppe; mit solchen Darstellungen werden wir uns später im 12. Kapitel noch eingehend zu beschäftigen haben.

Die $t_{\varkappa, \alpha}$ bilden die sogenannte **metazyklische Gruppe** (Kronecker). Auch alle ihre nichtzyklischen Teiler wollen wir als metazyklische Gruppen bezeichnen.

Die $t_{\varkappa, \alpha}$ liefern je nach der Wahl von $\varkappa$ und α folgende drei Typen:

Ist $\varkappa = 1$; $\alpha = 0$, dann wird $t_{1,0}$ die Einheitssubstitution.

Ist $\varkappa = 1$; $\alpha = 0$, dann ergibt $t_{1,\alpha}$ eine zyklische Substitution aller p Elemente, nämlich die Potenz s^{α}.

Ist $\varkappa > 1$, so erhält man eine Substitution, deren festbleibende Elemente z sich aus der Kongruenz

$$z \equiv \alpha + \varkappa z, \qquad z \equiv \frac{\alpha}{1 - \varkappa} \qquad (\operatorname{mod} p)$$

ergeben. Es bleibt also ein und nur ein Index ungeändert, d. h. ein und nur ein Element x_z wird nicht umgesetzt.

Die bewiesenen Eigenschaften sind charakteristisch für die metazyklischen Gruppen: **Metazyklische Gruppen sind solche transitive Gruppen von Primzahlgrad, deren Substitutionen überhaupt kein Element oder ein einziges oder alle ungeändert lassen.** Denn zunächst zeigt die Formel (8a) § 101, daß nur $(p-1)$ Substitutionen vorhanden sind, die kein Element ungeändert lassen; diese sind regulär, da sonst eine von 1 verschiedene Potenz mehr als ein Element nicht ändern würde; also enthält die Gruppe nur etwa unser s und seine Potenzen, d. h. H. Weiter folgt hieraus, daß jede Substitution der Gruppe den Teiler H in sich selbst transformiert; und so gelangen wir zu der oben hergeleiteten Gruppe.

Bilden wir die Potenz

$$t_{\varkappa, \alpha}^{\lambda} = \left| z, \ \alpha \frac{\varkappa^{\lambda} - 1}{\varkappa - 1} + \varkappa^{\lambda} z \right|, \qquad (\varkappa > 1)$$

so folgt, daß sie eine reguläre Substitution von $(p-1)$

Elementen wird; denn jeder Zyklus enthält u Elemente, falls $\varkappa$ zum Exponenten u (mod p) gehört, d. h. falls

$$\varkappa^u \equiv 1 \pmod{p} \qquad (u \min)$$

wird; u ist also ein Teiler von $(p-1)$. Ist $\varkappa$ eine primitive Wurzel modulo p, so hat $t_{\varkappa,\alpha}$ die Ordnung $(p-1)$ und besteht aus einem einzigen Zyklus.

Die gesamte metazyklische Gruppe ist durch die beiden Substitutionen

$$s = |z, z+1|, \quad t = |z, \varkappa z|$$

bestimmt; ihre metazyklischen Teiler durch die beiden Substitutionen

$$s = |z, z+1|, \quad t^\omega = |z, \varkappa^\omega z|,$$

wenn $\varkappa$ eine primitive Wurzel modulo p bedeutet, und ω ein Faktor von $(p-1)$ ist.

Gehen wir mit diesen Ergebnissen zu den transitiven Gruppen G des Primzahlgrades p zurück, so können wir jetzt sagen, daß die Zwischengruppe J zu jedem zyklischen Teiler H von G der Klasse p eine metazyklische Gruppe wird. Ist in (10) der Wert $\varkappa = 0$, also H eine selbstkonjugierte Untergruppe von G, dann ist G selber eine metazyklische Gruppe; und solche Gruppen bestehen für jeden Divisor q von $(p-1)$.

Ein tieferes Eindringen in die einschlägigen Verhältnisse führt noch zu weiteren interessanten Ergebnissen, von denen wir die folgenden ohne Beweise hier anführen wollen:

Bei allen Gruppen G mit $q = 1$ [in der Formel (10)] ist $\varkappa = 0$; auch bei $q = 2$ und $p = 4n - 1$ ist $\varkappa = 0$.

Jede transitive Gruppe von Primzahlgrad, die nicht metazyklisch ist, muß mindestens zweifach transitiv sein.

Es gibt unter den transitiven Gruppen des Primzahlgrades p nur vier, bei denen $\varkappa = 1$ ist, die also genau $(p+1)$ Teiler der Ordnung p enthalten. Dies sind die symmetrische und die alternierende Gruppe des Grades 5, eine Gruppe des Grades 7 und der Ordnung 168 und eine Gruppe des Grades 11 und der Ordnung 660.

§ 104. Aus § 96, S. 123 entnehmen wir, daß, wenn G eine $(k+1)$-fach transitive Gruppe des Grades $(n+1)$ und H ein Teiler von G ist, der eins der Elemente von G ungeändert läßt, daß dann dieses H noch k-fach transitiv bleibt, und daß dabei die Ordnung von G genau $(n+1)$ mal größer als die von H ist. Dagegen gilt nicht allgemein der umgekehrte Satz, daß jede k-fach transitive Gruppe H von n Elementen als Teiler in einer $(k+1)$-fach transitiven Gruppe von $(n+1)$ Elementen mit $(n+1)$-mal so hoher Ordnung enthalten ist.

Wir wollen untersuchen, wann die Umkehrung gestattet ist. Wir setzen voraus, G und H erfüllten die Forderungen. Die Elemente der k-fach transitiven Gruppe H seien x_1, $x_2, x_3, \ldots, x_n$; in G komme noch das Element x_{n+1} dazu. G ist $(k+1)$-fach und mindestens zweifach transitiv; die Ordnung von G durch $(n+1)n$ also durch 2 teilbar. Nach dem Cauchyschen Satze hat G einen Teiler der Ordnung 2 und daher eine Substitution g', die nur Zyklen der Ordnung 2 enthält; $(x_\sigma x_\tau)$ sei ein Zyklus von g'. Wegen der mindestens zweifachen Transitivität hat G eine Substitution t mit den Folgen $x_\sigma x_{n+1}$ und $x_\tau x_1$. Transformiert man g' durch t, so erhält man ein auch in G vorkommendes g_1 der Ordnung 2 mit dem Zyklus $(x_{n+1} x_1)$.

Ferner gibt es in H Substitutionen mit der Folge $x_1 x_\alpha$

$$h_\alpha = (\ldots x_1 x_\alpha \ldots) \ldots \qquad (\alpha = 2, 3, \ldots, n)$$

also in G, da H das Element x_{n+1} nicht umstellt, neben

$$g_1 = (x_{n+1} x_1) \ldots$$

noch je ein g_α der Ordnung 2, wo

$$g_\alpha = h_\alpha^{-1} g_1 h_\alpha = (x_{n+1} x_\alpha) \ldots \qquad (\alpha = 2, 3, \ldots, n).$$

Mit Hilfe der g_α wird die Zerlegung von G geliefert

$$G = H + Hg_1 + Hg_2 + Hg_3 + \ldots + Hg_n,$$

wobei der Komplex Hg_α alle und nur die Substitutionen von G mit der Folge $x_{n+1} x_\alpha$ enthält. Weiter folgt

$$G = H + Hg_1 + H h_2^{-1} g_1 h_2 + H h_3^{-1} g_1 h_3 + \ldots$$
$$= H + Hg_1 h_1 + Hg_1 h_2 + Hg_1 h_3 + \ldots + Hg_1 h_n$$

mit $h_1 = 1$, und daraus, daß jede Substitution von G entweder zur Gruppe H oder zu einem der Komplexe

$$H g_1 h_\alpha \qquad (\alpha = 1, 2, 3, \ldots, n)$$

gehört. Da andererseits $\{H, g_1\}$ ein Teiler von G ist, so wird

$$G = \{H, g_1\}.$$

Sind die abgeleiteten notwendigen Bedingungen zwischen G, H und g_1 auch hinreichend? Um das zu untersuchen, nehmen wir H und $g_1 = (x_{n+1} x_1) \ldots$ als gegeben an. Dann können wir wie oben die Substitutionenreihe $h_1, h_2, \ldots, h_\alpha, \ldots, h_n$ mit den Folgen $x_{n+1} x_1$; $x_{n+1} x_2$; $\ldots$, $x_{n+1} x_\alpha$, $\ldots$, $x_{n+1} x_n$ bilden. Wir setzen nun voraus, es sei möglich, wenn h', h'', h''', ... beliebige Substitution aus H bedeuten, jedes Produkt $g_1 h' g_1$ entweder in der Form h'' oder in der Form $h'' g_1 h'''$ darzustellen; dann kann man jedes Produkt $g_1 h' g_1 h'' g_1 h''' \ldots$ auf ein $h^{(\Gamma)}$ oder auf ein $h^{(\sigma)} g_1 h^{(\tau)}$ reduzieren, wie z. B.

$$\begin{aligned} g_1 h' g_1 h'' g_1 h''' &= h^{IV} g_1 h^{V} \cdot h'' g_1 h''' \\ &= h^{IV} \cdot g_1 h^{VI} g_1 \cdot h''' \\ &= h^{IV} h^{VII} g_1 h^{VIII} h''' = \ldots \\ &= h^{(\sigma)} g_1 h^{(\tau)}. \end{aligned}$$

Demnach kann jede Substitution von $\{H, g_1\}$ auf eine der beiden Formen

$$h' \quad \text{oder} \quad h' g_1 h''$$

gebracht werden. Dabei enthält, wie leicht zu sehen ist, $h' g_1 h''$ alle und auch nur die Substitutionen, die das x_{n+1} in das gleiche Element wie h'' das x_1 überführen. Die zweite Form $h' g_1 h''$ kann noch vereinfacht werden. Setzt nämlich h_α das Element x_1 in derselben Weise um wie h'', so läßt das Produkt

$$g_1 h_\alpha h''^{-1} g_1 h'^{-1}$$

das Element x_{n+1} ungeändert, wird also $= (h''')^{-1}$ gesetzt werden können. Daraus folgt wegen $g_1^2 = 1$ die Darstellung

$$h' g_1 h'' = h''' g_1 h_\alpha,$$

wo der dritte Faktor rechts der Reihe $h_2, h_3, \ldots, h_n$ angehört. Demnach wird wegen $H h''' = H$

$$\{H, g_1\} = H + H g_1 + H g_1 h_2 + H g_1 h_3 + \ldots + H g_1 h_n ,$$

und die Ordnung von $\{H, g_1\}$ ist das $(n+1)$-fache der Ordnung von H. Ferner ist die Gruppe $\{H, g_1\}$ genau $(k+1)$-fach transitiv. Gehört nämlich x_{n+1} zu den Elementen, für die eine Folge $x_\alpha x_{n+1}$ vorgeschrieben ist, so befriedigt zuerst eins der $g_1, g_2, \ldots, g_n$, etwa g_α, diese eine Forderung. Die weiteren k Forderungen, die im allgemeinen durch diese erste Operation modifiziert worden sind, befriedigt man dann durch eine passende rechtsseitig an g_α angefügte Substitution aus H. Gehört dagegen x_{n+1} nicht zu den Elementen, für die eine Folge vorgeschrieben ist, so kann man es durch die Transformation aller Folgen mit einem der g_α dazu machen. Die transformierten Bedingungen lassen sich dann befriedigen, wie eben gezeigt worden ist. Endlich kann man die Transformation rückgängig machen.

Sonach ist $\{H, g_1\}$ das verlangte G von $(k+1)$-facher Transitivität und vorgeschriebener Ordnung.

Will man die Bedingungen bei gegebenem g_1, d. h.

$$g_1 h' g_1 = h'' g_1 h''' \tag{11}$$

prüfen, so muß man für h' sämtliche Substitutionen der Gruppe H einsetzen und h'' und h''' zu bestimmen suchen.

§ 105. Um die im vorigen Paragraphen besprochenen Verhältnisse zu erläutern, wollen wir an die zweifach transitive metazyklische Gruppe von 5 Elementen anknüpfen. Sie ist von der Ordnung 20 und wird durch das folgende Schema dargestellt, in dem nur die Indizes der Elemente in die Klammern gesetzt sind:

(H)

1	(1243)	(14) (23)	(1342)
(12345)	(1452)	(13) (45)	(2453)
(13524)	(2354)	(12) (35)	(1435)
(14253)	(1325)	(25) (34)	(1254)
(15432)	(1534)	(15) (24)	(1523).

Diese Substitutionen bilden die Gruppe H; sie ist durch zwei erzeugende Substitutionen darstellbar,

$$H = \{(12345), (1243)\} = \{h_1, h_2\}.$$

Als g_1 nehmen wir versuchsweise die Substitution zweiter Ordnung

$$g_1 = (16)(25)$$

und prüfen das Bestehen der Relationen (11). Zuerst sei $h' = h_1$. Dann wird gefordert

$$(16)(25) \cdot (12345) \cdot (16)(25) = (26534) = h'' \cdot (16)(25) \cdot h'''.$$

Die linke Seite liefert die Folge 65; da h'' das Element 6 nicht umsetzt, muß h''' die Folge 15 enthalten. Also entnehmen wir aus der Tabelle für H, daß h''' nur eine der vier Substitutionen mit der Folge 15, nämlich

$$(15432), (1534), (15)(24), (1523)$$

sein kann. Wir untersuchen die erste Möglichkeit. (11) fordert

$$(26534) = h''(16)(25) \cdot (15432) = h'' \cdot (165)(243),$$

$$h'' = (26534) \cdot (156)(234) = (15432) = h_1^4,$$

so daß

$$g_1 h_1 g_1 = h_1^4 g_1 h_1^4$$

wird. Daraus liefert der Übergang zu den Reziproken

$$g_1 h_1^4 g_1 = h_1 g_1 h_1.$$

Nach derselben Methode ergibt sich die weitere Reihe von Gleichungen

$$g_1 h_1^2 g_1 = h_2^2 g_1 h_1^2; \qquad g_1 h_1^3 g_1 = h_1 h_2^2 g_1 h_1^3;$$
$$g_1 h_2 g_1 = h_1^4 h_2^3 g_1 h_1^4; \qquad g_1 h_2^2 g_1 = h_1^2 g_1 h_1^3;$$
$$g_1 h_2^3 g_1 = h_1^2 h_2^3 g_1 h_1^2; \quad g_1 h_1 h_2 g_1 = h_1^3 h_2 g_1 h_1^3; \quad \ldots$$

und so sieht man, daß in allen Fällen (11) erfüllt ist. Folglich besteht eine dreifach transitive Gruppe des Grades 6 und der Ordnung 120 mit drei erzeugenden Substitutionen

$$G = \{(16)(25), (12345), (1243)\},$$

die H als den Teiler enthält, der das Element 6 nicht umstellt.

Dagegen gibt es keine Gruppe F vom Grade 7 bei vierfacher Transitivität, die G in ähnlicher Weise enthält. Denn nach dem Satze § 100, S. 129 fällt bei $k = 4$ ein F, das Substitutionen von 4 Elementen enthält, mit der alternierenden oder der symmetrischen zusammen, und sein Index zu G ist >7.

§ 106. Wir wollen noch einiges über intransitive Gruppen beibringen.

Zunächst über die Ordnung solcher Gruppen. Zerfallen die Elemente in $\varkappa$ transitiv verbundene Systeme der Grade $n_1, n_2, \ldots, n_\varkappa$, wo jedes $n_\alpha \geqq 1$ ist, dann wird die Ordnung der Gruppe ein Teiler von $(n_1!\, n_2! \ldots n_\varkappa!)$. Die höchsten Ordnungen entstehen, wenn $\varkappa = 2$ und $n_1 = n - 1$, $n_2 = 1$ und wenn $n_1 = n - 2$, $n_2 = 2$ wird. Dann ist $r = (n-1)!$ bzw. $r = 2(n-2)!$ das Maximum.

Für unsere weiteren Untersuchungen auf dem Gebiete der transitiven und intransitiven Gruppen beschränken wir uns auf solche intransitive Gruppen G, deren Elemente in nur zwei Systeme zerfallen, die einzeln transitiv sind. Es seien

$$x_1, x_2, \ldots, x_n; \quad \xi_1, \xi_2, \ldots, \xi_\nu$$

die Elemente von G; die Substitutionen der Gruppe G sollen die x_α unter sich und die ξ_α unter sich transitiv verbinden; dagegen sollen sie die x_α nicht mit den ξ_α verbinden. Wir betrachten die Untergruppe S von G, die nur die x_α umsetzt, alle ξ_α aber an ihren Stellen läßt. S ist selbstkonjugiert in G. Mit Hilfe von S zerlegen wir G in S und seine Nebenkomplexe

$$G = S + g_2 S + g_3 S + \ldots + g_m S;$$

dann setzen alle Substitutionen von $g_\alpha S$ die ξ in derselben Weise um und nur sie in eben dieser Weise. S und seine Nebenkomplexe bilden eine zu G isomorphe Gruppe, und zwar ist G zu S genau s-stufig isomorph, wenn s die Ordnung von S bedeutet. Diese isomorphe Gruppe mag D heißen.

Ferner betrachten wir den selbstkonjugierten Teiler Σ von G, der nur die ξ_α umsetzt, aber die x_α an ihren Stellen läßt. Mit Σ finden wir die Zerlegung

$$G = \Sigma + g_2'\Sigma + g_3'\Sigma + \ldots + g_\mu'\Sigma$$

und kommen durch Σ und seine Nebenkomplexe gleichfalls auf eine zu G isomorphe Gruppe, die wir Δ nennen. G ist zu Δ in σ-stufigem Isomorphismus, wenn σ die Ordnung von Σ angibt.

Nun nehmen wir die folgende Zuordnung zwischen den Operatoren oder den Substitutionen von S und von Σ vor. Jeder Substitution von Σ entspricht eine aus G und dieser entsprechen s aus S; diese s aus S ordnen wir jener einen aus Σ zu. Umgekehrt entspricht jeder Substitution von S eine aus G, und dieser einen σ aus Σ, die wir wieder der einen aus S zuordnen. Dann sieht man, daß ein gewisser allgemeinerer Isomorphismus zwischen S und Σ festgelegt ist, der den bisher benutzten als Sonderfall enthält: je σ Operatoren der einen Gruppe Σ entsprechen s der anderen Gruppe S und umgekehrt, derart, daß den Produkten zweier das Produkt der entsprechenden entspricht.

Der einfachste Fall ist der durch $s = \sigma = 1$ gegebene. Bei ihm sind S und Σ einstufig isomorph. Nimmt man dabei die ξ_α von den x_α verschieden an und multipliziert je zwei einander durch den Isomorphismus der ξ und der x zugeordnete Substitutionen, so erhält man die einfachsten intransitiven Gruppen.

§ 107. G sei eine transitive Gruppe der Elemente $x_1, x_2, x_3, \ldots, x_n$ und h eine Substitution der gleichen Elemente. Diese Substitution h möge mit allen Substitutionen von G vertauschbar sein. Gesetzt nun, h ließe das Element x_1 ungeändert, so sei g_0 eine Substitution von G mit der Folge $x_1 x_\alpha$, dann würde, weil $g_0^{-1} h g_0 = h$ ist, h auch x_α nicht umsetzen, also müßte, da $\alpha = 1, 2, 3, \ldots, n$ sein kann, $h = 1$ werden. Ist h von der Einheit verschieden, so setzt es somit alle Elemente um. In diesem Falle muß h regulär sein, weil sonst eine Potenz $h^\varkappa$, ohne $= 1$ zu werden, Elemente an ihren Platz ließe, während doch mit h zugleich auch $h^\varkappa$ mit allen Substitutionen von G vertauschbar ist.

Ist jetzt H der Komplex aller mit den Substitutionen von G vertauschbaren Substitutionen, so ist offenbar H eine Gruppe aus regulären Substitutionen. Die Ordnung einer solchen Gruppe H ist höchstens gleich ihrem Grade n. Denn wäre ihre Ordnung größer als n, so gäbe es in ihr

zwei verschiedene Substitutionen $h_1\, h_2$ mit einer gleichen Folge $x_1\, x_\alpha$, also auch das nicht identische Produkt $h_1\, h_2^{-1}$, das x_1 nicht umsetzt.

Sind alle Substitutionen von H mit allen von G vertauschbar, so enthalten H und G nur reguläre Substitutionen ihrer n Elemente, und die Ordnungen von H und G sind gleich n, falls G und H dieselben Elemente haben und beide transitiv sind.

§ 108. Ist eine transitive Substitutionengruppe eine Abelsche, so ist sie in regulärer Form, d. h. ihre Ordnung ist ihrem Grade gleich (§ 18, S. 28). Enthält nämlich eine ihrer Substitutionen s_1 das Element x_1 nicht, $s_1 = (x_1)(x_2 \ldots) \ldots$, so nehmen wir eine zweite Substitution der Gruppe s_k, die x_1 in x_k überführt, $s_k = (x_1 x_k \ldots) \ldots$ und bilden

$$s_1 = s_k^{-1} \cdot s_1 \cdot s_k = (x_k)(x_2 \ldots) \,.$$

Hieraus sieht man, daß s_1 auch das Element x_k nicht enthält; und da k beliebig ist, so wird $s_1 = 1$. Also ist die Gruppe regulär. Dieser Satz kann auch als besonderer Fall des vorigen, $G = H$, aufgefaßt werden.

§ 109. In § 18, S. 28 haben wir aus dem Cayleyschen Quadrate einer abstrakten Gruppe G eine ihr einstufig isomorphe Substitutionengruppe S hergeleitet, die, wenn kurz durch das Schema

$$\begin{array}{c|cc} & 1 & a \\ \hline g & g & ga \end{array}$$

das Cayleysche Quadrat bezeichnet wird, als

$$s_g = \begin{pmatrix} g\,a \\ a \end{pmatrix}; \qquad S = [s_g]$$

geschrieben werden kann.

Vertauscht man Zeilen und Spalten des Cayleyschen Quadrates, so entsteht eine zweite Gruppe Σ, die einstufig isomorph zu G, also auch zu S ist, und aus

$$\sigma_g = \begin{pmatrix} a\,g \\ a \end{pmatrix}; \qquad \Sigma = [\sigma_g]$$

gebildet wird. Dann behaupten wir, daß alle s_g mit allen σ_g vertauschbar sind. Es ist in der Tat

$$\sigma_h^{-1} s_g \sigma_h = \begin{pmatrix} a \\ a\,h \end{pmatrix} \begin{pmatrix} g\,a \\ a \end{pmatrix} \begin{pmatrix} a\,h \\ a \end{pmatrix} = \begin{pmatrix} a \\ a\,h \end{pmatrix} \begin{pmatrix} g\,a\,h \\ a\,h \end{pmatrix} \begin{pmatrix} a\,h \\ a \end{pmatrix} = \begin{pmatrix} a \\ a\,h \end{pmatrix} \begin{pmatrix} g\,a\,h \\ a \end{pmatrix}$$

$$= \begin{pmatrix} g\,a \\ g\,a\,h \end{pmatrix} \begin{pmatrix} g\,a\,h \\ a \end{pmatrix} = \begin{pmatrix} g\,a \\ a \end{pmatrix} = s_g \,.$$

Also erfüllen S und Σ die Bedingungen des Satzes in § 107, und beide Gruppen haben dieselbe Ordnungs- und Gradzahl n. Die transitiven Gruppen regulärer Substitutionen sind einander paarweise derart zugeordnet, daß die eine aus allen den Substitutionen besteht, die mit denen der anderen Gruppe vertauschbar sind.

---

10. Kapitel.

Substitutionengruppen. — Primitivität.

§ 110. Lassen sich die Elemente einer transitiven Gruppe G so in Systeme zerlegen, daß jede Substitution von G, die eins der Elemente des einen Systems in ein Element eines zweiten Systems überführt, alle Elemente des ersten in alle jenes zweiten überführt (wobei das zweite System mit dem ersten zusammenfallen kann), so heißt die Gruppe imprimitiv. Ist bei einer transitiven Gruppe eine solche Einteilung nicht möglich, so heißt die Gruppe primitiv. Bei mehrfacher Transitivität ist natürlich die Gruppe stets primitiv; Imprimitivität ist nur bei einfachtransitiven Gruppen möglich.

Aus der Definition der Imprimitivität folgt sofort, daß alle Systeme gleich viele Elemente umfassen; sowie, daß jede Substitution der imprimitiven Gruppe G durch eine Umstellung der Systeme untereinander und mit darauffolgenden Umstellungen der Elemente der einzelnen Systeme bewirkt werden kann. Die Substitutionen, welche die Systeme sämtlich ungeändert lassen, bilden einen selbstkonjugierten Teiler H von G. Ist s seine Ordnung, so teilen sich die Substitutionen in Teile von je s, so daß alle des gleichen Teils die Systeme der Imprimitivität in gleicher Weise umstellen. Das folgt aus der Zerlegung

$$G = H + g_2 H + g_3 H + \dots + g_n H$$

ohne jede Schwierigkeit.

§ 111. I. Lassen sich aus den Elementen x_1, x_2, ..., x_n der Gruppe G a herausheben x'_1, x'_2, ..., x'_a, so daß jede Substitution von G, die auf ein x' ein zweites x' folgen läßt, alle x' untereinander vertauscht, so ist G imprimitiv. Es sei H der Teiler von G, der nur die x' untereinander vertauscht; t_2 eine nicht zu H gehörige Substitution. Dann führen alle Substitutionen des Komplexes $H t_2$ alle x' in a neue x'' über; denn würde durch $H t_2$ ein x'_α in ein x'_β umgewandelt, dann würden es alle. Und nur die $H t_2$ führen die x' in die x'' über. Denn tut dies ein u, so würde $u \cdot t_2^{-1}$ zu H gehören, also u zu $H t_2$. Geht man so fort, dann erkennt man die Imprimitivität von G.

II. G ist auch schon imprimitiv, wenn jede Substitution, die auf ein bestimmtes Element x'_1 ein x' folgen läßt, alle x' untereinander vertauscht. Denn wenn u die Folge $x'_\alpha x'_\beta$ hat und t die Folge $x'_1 x'_\alpha$, so wird das Produkt $t u$ auf x'_1 folgen lassen x'_β, also alle x' aufeinander. Und da der Faktor t dies tut, so tut der Faktor u das Gleiche. Damit ist der Satz auf den vorigen zurückgeführt.

Mit diesem ersten Satze sind die beiden folgenden Theoreme im Wesen identisch. Wir können daher wohl ihre Beweise übergehen.

III. Lassen sich aus den Elementen x_1, x_2, ..., x_n der transitiven Gruppe G zwei Komplexe x'_1, x'_2, ..., x'_a und x''_1, x''_2, ..., x''_a herausheben, derart, daß jede Substitution von G, die auf ein x' ein x'' folgen läßt, alle x' in alle x'' umwandelt, so ist G imprimitiv.

IV. Wie man auch aus den Elementen x_1, x_2, ..., x_n einer primitiven Gruppe G a Elemente x'_1, x'_2, ..., x'_a auswählt, die Gruppe enthält stets Substitutionen, die eins der x' in ein anderes x' und gleichzeitig ein drittes x' in eins der übrigen $(n-a)$ Elemente umwandelt.

Aus dem Satze I können wir schließen:

V. Ist G eine primitive Gruppe der n Elemente x_1, x_2, ..., x_n, und H der Teiler von G, der x_1 nicht umsetzt, so läßt H keins der anderen Elemente x_2, x_3, ..., x_n ungeändert; mit anderen

Worten: so gibt es in H Substitutionen, die x_2, solche die $x_3, \ldots$, solche die x_n umstellen. Gesetzt, alle Substitutionen von H ließen $x_1, x_2, \ldots, x_\alpha$ und nur diese Elemente auf ihren Plätzen, so wählen wir aus G eine Substitution s_0 mit der Folge $x_2 x_1$; dann läßt $s_0^{-1} H s$ das Element x_1 ungeändert; daher ist $s_0^{-1} H s_0 = H$, und s_0 wandelt die $x_2, x_3, x_4, \ldots, x_\alpha$ als festbleibende Elemente untereinander um. Nach dem Theorem II wäre dann aber G imprimitiv.

§ 112. Sind bei einer imprimitiven Gruppe Einteilungen der Elemente in Systeme der Imprimitivität auf zweierlei Arten möglich, so kann man eine dritte Einteilung dadurch herleiten, daß man alle Elemente, die ein System der ersten mit einem Systeme der zweiten Einteilung gemeinsam hat, zu einem Systeme der dritten Einteilung vereinigt.

In der Tat wandeln ja alle Substitutionen der Gruppe, die ein Element eines Systems der dritten Einteilung in eins des gleichen Systems überführen, wie man sofort sieht, alle dieses Systems in ebensolche um. Gleichzeitig bemerkt man, daß die Anzahl der Elemente jedes dritten Systems ein gemeinsamer Teiler der Elementenzahl der Systeme der beiden ersten Einteilungen wird. Sind also diese beiden Anzahlen teilerfremd zueinander, so ist eine dritte Einteilung auf diesem Wege nicht zu erreichen.

Die Umkehrung des obigen Satzes, die sich auf die Zusammenfassung von Systemen der Imprimitivität zu allgemeineren beziehen würde, findet nur in eingeschränkter Weise statt, wie das Beispiel

$$G = \{(x_1 x_2)(x_3 x_4)(x_5 x_6),\ (x_1 x_4 x_5)(x_2 x_6 x_3)\}$$

zeigt. Hier sind die beiden Einteilungen

$$x_1 x_2;\ x_3 x_5;\ x_4 x_6 \quad \text{und} \quad x_1 x_3;\ x_2 x_4;\ x_5 x_6$$

möglich, eine Zusammenfassung dagegen nicht.

§ 113. Die Frage nach den Maximalordnungen imprimitiver Gruppen gegebenen Grades n läßt sich leicht beantworten. Zerfallen die n Elemente in $\varkappa$ Systeme von je λ Elementen, so gibt es im höchsten Falle $\varkappa!$ Permutationen der Systeme; und für die Elemente jedes ein-

zelnen Systems $\lambda!$, also zusammen im Maximum $\varkappa!(\lambda!)^\varkappa$, wobei $\varkappa \cdot \lambda = n$ sein muß. So enthält man Gruppen von einer der Ordnungen

$$2!\left(\frac{n}{2}!\right)^2, \quad 3!\left(\frac{n}{3}!\right)^3, \quad 4!\left(\frac{n}{4}!\right)^4, \quad \ldots$$

und man erkennt leicht, daß die erste der angegebenen Anzahlen das Maximum der Ordnungen liefert.

§ 114. Ist H ein selbstkonjugierter Teiler der primitiven Gruppe G, so ist H transitiv. Insbesondere ist H transitiv, wenn G mehrfach transitiv ist.

Wäre nämlich $x_1, x_2, \ldots, x_a$ ein System transitiv in H verbundener Elemente, die durch H mit keinem der anderen Elemente $x_{a+1}, \ldots, x_n$ zusammenhängen $(a < n)$, so wählen wir in G eine Substitution s_0, die eins der Elemente $x_1, x_2, \ldots, x_a$ in ein anderes desselben Systems, und ein drittes in eins der Elemente $x_{a+1}, \ldots, x_n$ umwandelt. Wegen der Primitivität von G gibt es ein solches s_0 in G. Weil nun $s_0^{-1} H s_0 = H$ wird, so folgt, daß H mehr als die a Elemente $x_1, x_2, \ldots, x_a$ transitiv miteinander verbindet. Also muß $a = n$ werden.

Aus dem bewiesenen Satze folgt, daß, wenn eine transitive Gruppe G einen selbstkonjugierten, intransitiven Teiler H besitzt, dann G eine imprimitive Gruppe ist.

Die Anzahl der intransitiven Elementensysteme, in die die Elemente von H zerfallen, ist ein Divisor des Grades von G. Als Beispiel diene folgendes: Die Gruppe, die aus

$$1, \ (x_1 x_2 x_3 x_4), \ (x_1 x_3)(x_2 x_4), \ (x_1 x_4 x_3 x_2)$$

besteht, hat die Gruppe $[1, (x_1 x_3)(x_2 x_4)]$ als intransitiven selbstkonjugierten Teiler; und sie selbst ist imprimitiv mit den Systemen x_1, x_3 und x_2, x_4 oder auch x_1, x_2 und x_3, x_4.

Eine Vervollständigung des Theorems liefert der folgende Satz, auf dessen Beweis wir nicht eingehen wollen: Ein selbstkonjugierter Teiler einer k-fach transitiven Gruppe des Grades n, bei $2 < k < n$, ist im allgemeinen mindestens $(k-1)$-fach transitiv. Eine Ausnahme können nur dreifach transitive

Gruppen des Grades 2^m mit selbstkonjugierten Gruppen der Ordnung 2^m als Teiler bilden. (Jordan; Burnside.)

§ 115. Wir beweisen nun folgendes Theorem:

Besitzt die primitive Gruppe G des Grades n Substitutionen von weniger als n Elementen, ist also ihre Ordnung größer als n, dann besitzt G auch einen Teiler genau vom Grade $(n-1)$; oder in anderer Weise ausgedrückt: Eine transitive Gruppe G des Grades n, die keinen Teiler enthält, der genau $(n-1)$ Elemente umsetzt, jedoch Teiler geringeren Grades, ist imprimitiv.

Der Voraussetzung nach besitzt G einen Teiler L von $\lambda < n$ Elementen. Diese Elemente wollen wir mit $x_1, x_2, \ldots, x_\lambda$ bezeichnen. Wir nehmen zuerst $\lambda < \frac{n}{2}$ an; dann gibt es zufolge der Primitivität von G in dieser Gruppe eine Substitution s_α, die auf eins der Elemente von L ein anderes derselben, auf ein zweites von L dagegen ein neues, nicht in L vorkommendes Element folgen läßt. Dann enthält $L_1' = s_\alpha^{-1} L s_\alpha$ neben alten Elementen von L zugleich neue, so daß $L_1 = \{L, L_1'\}$ mehr als λ, aber weniger als $2\lambda < n$ Elemente aufweist. Ist ihre Anzahl λ_1 auch noch $< \frac{n}{2}$, so kann man mit Hilfe einer zweiten Substitution s_β zu einem neuen Teiler $L_2 = \{L_1, s_\beta^{-1} L_1 s_\beta\}$ mit einer noch größeren Anzahl von Elementen etwa mit λ_2 gelangen, usf. Es sei nun diese Zahl λ_2 schon gleich oder größer als $\frac{n}{2}$, und die Elemente von L_2 seien $x_1, x_2, \ldots, x_{\lambda_2}$. Dann gibt es, wiederum wegen der Primitivität von G, eine Substitution s_γ, die auf eins der nicht in L_2 vorhandenen Elemente ein anderes nicht in L_2 vorhandenes, dagegen auf ein zweites nicht in L_2 vorhandenes ein in L_2 vorhandenes folgen läßt. Dann verbindet $L_3' = s_\gamma L_2 s_\gamma^{-1}$ mit $x_1, x_2, \ldots, x_{\lambda_2}$ neue Elemente, aber ein neues bleibt bei der festgesetzten Wahl von s_γ außerhalb der Gruppe L_3'; und endlich enthält L_3', da $\lambda_2 \geqq \frac{n}{2}$ ist, auch noch alte Elemente; folglich besitzt $L_3 = \{L_2, L_3'\}$ wiederum mehr

Elemente als L_2, aber weniger als G selbst. Fährt man so fort, dann gelangt man zu einer Gruppe L_ν von genau $(n-1)$ Elementen, deren Existenz behauptet war.

Im Anschluß hieran wollen wir unter Beihehaltung der gleichen Bezeichnungen beweisen:

Enthält eine primitive Gruppe G des Grades n einen transitiven Teiler L von weniger als n Elementen, so ist G mindestens zweifach transitiv. Denn mit L werden $L_1, L_2, \ldots, L_\nu$ transitiv, und aus der Transitivität von L_ν folgt die Behauptung (§ 98). Ist n eine Primzahl, so ist die Gruppe G stets primitiv, sobald sie transitiv ist, da eine Einteilung der Elemente in Systeme von gleichvielen Gliedern nicht möglich ist, falls jedes System mehr als ein Element enthalten soll.

§ 116. Eine jede transitive reguläre Gruppe ist imprimitiv. Jede ihrer Substitutionen gibt Veranlassung zur Bildung eines Systems der Imprimitivität, indem man aus allen Elementen eines jeden Zyklus ein System bildet. Machen wir nämlich alle Elemente $x_1, x_2, \ldots, x_a$ eines Zyklus der Substitution s zu einem Systeme, so reicht es aus, zu beweisen, daß jede Substitution, die eins dieser Elemente in eins derselben umwandelt, alle diese nur untereinander vertauscht. x_λ sei eins unter ihnen, und die Substitution t der Gruppe habe die Folge $x_1 x_\lambda$; dann hat eine Potenz s^ν von s dieselbe Folge, und $t \cdot s^{-\nu}$ läßt x_λ ungeändert. Wegen der Regularität ist $t \cdot s^{-\nu} = 1$ und $t = s^\nu$. Also vertauscht t alle $x_1, x_2, \ldots, x_a$ nur untereinander, und diese Elemente bilden daher ein Imprimitivitätssystem.

§ 117. Wir haben in § 99, S. 127 die folgenden Sätze bewiesen: Enthält eine $k(>1)$-fach transitive Gruppe eine Transposition, so ist sie symmetrisch; enthält sie eine Zirkularsubstitution dritter Ordnung, so ist sie alternierend oder symmetrisch. Für einfache Transitivität gelten diese Sätze nicht mehr unbedingt, wie die Gruppen des Grades 4

$$1,\quad (x_1 x_2)(x_3 x_4),\quad (x_1 x_3)(x_2 x_4),\quad (x_1 x_4)(x_2 x_3),$$
$$(x_1 x_2),\quad (x_3 x_4),\quad (x_1 x_4 x_2 x_3),\quad (x_1 x_3 x_2 x_4)$$

und des Grades 6

$$G = \{(x_1 x_2 x_3),\quad (x_4 x_5 x_6),\quad (x_1 x_4)(x_2 x_5)(x_3 x_6)\}$$

zeigen. Dagegen gelten die Sätze auch bei einfacher Transitivität für primitive Gruppen, wie jetzt bewiesen werden soll.

G sei eine primitive Gruppe der Elemente x_1, x_2, x_3, ..., x_n, und $s_1 = (x_1 x_2)$ eine in G vorkommende Transposition. Dann enthält (§ 111, IV, S. 143) G Substitutionen, die eins der Elemente x_1, x_2 in sich oder in das andere und das zweite der Elemente x_1, x_2 in ein neues x_3 umwandeln; $t_1 = (x_1 x_1) \dots (x_2 x_3 \dots)$ sei eine solche Substitution. Dann ist $t_1^{-1} s_1 t_1 = (x_1 x_3)$ und die symmetrische Gruppe $H_3 = \{(x_1 x_2), (x_2 x_3)\}$ von x_1, x_2, x_3 in G enthalten. Weiter gibt es in G Substitutionen, die eins der Elemente x_1, x_2, x_3 in sich oder in ein anderes unter ihnen, aber ein zweites der Elemente x_1, x_2, x_3 in ein neues x_4 umwandeln; $t_2 = (x_2 x_1 \dots) \dots (x_3 x_4 \dots) \dots$ sei eine solche Substitution. In H_3 kommt dann $(x_2 x_3)$ vor und in G die Transformierte $t_2^{-1}(x_2 x_3) t_2 = (x_1 x_4)$. Daher ist die symmetrische Gruppe $H_4 = \{(x_1 x_2), (x_1 x_3), (x_1 x_4)\}$ ein Teiler von G. Geht man so weiter, so erkennt man die Richtigkeit des Satzes.

In ähnlicher Art geht man beim Beweise des zweiten Satzes vor. Hier sei $s_1 = (x_1 x_2 x_3)$ eine in G vorkommende Zirkularsubstitution dritter Ordnung. Nun enthält G Substitutionen, die eins der Elemente x_1, x_2, x_3 in sich oder in ein anderes, und ein zweites derselben Elemente in ein neues x_4 umwandelt. Eine solche Substitution sei z. B. $t_1 = (x_1 x_2 x_5 \dots) \dots (x_3 x_4 \dots) \dots$; dann wird

$$t_1^{-1}(x_1 x_2 x_3) t_1 = (x_2 x_5 x_4) = \sigma ,$$

$$s_1^2 \sigma s_1 \sigma^2 s_1 = (x_1 x_2 x_4) ,$$

und G enthält außer $(x_1 x_2 x_3)$ noch die Zirkularsubstitution $(x_1 x_2 x_4)$, und die alternierende Gruppe von x_1, x_2, x_3, x_4 ist als Teiler in G enthalten (vgl. den Beweis zu § 99). Die Fortsetzung dieses Verfahrens führt zum behaupteten Satze. So folgt: Enthält eine primitive Gruppe eine Transposition, so ist sie symmetrisch; enthält eine primitive Gruppe eine Zirkularsubstitution aus drei Elementen, so ist sie alternierend oder symmetrisch.

§ 118. Gesetzt, es ist eine auflösbare, primitive

Substitutionengruppe G gegeben. Das letzte Glied der Hauptreihe vor der Einheit wird (§ 58, S. 76) eine Abelsche Gruppe H der Ordnung p^α, wobei p eine Primzahl bedeutet. Nach § 114, S. 145 ist H transitiv in den Elementen von G; und nach § 97, S. 125 ist die Ordnung einer transitiven Gruppe ein Vielfaches ihres Grades. In unserem Falle ist demnach der Grad von H und damit auch der von G eine Potenz der Primzahl p. D. h.: Eine auflösbare Gruppe kann nur dann primitiv sein, wenn ihr Grad eine Primzahlpotenz ist.

§ 119. Die Gruppe G der Ordnung $r = n \cdot s$ möge die Gruppe H der Ordnung s als Teiler enthalten. Dann kann man mit Hilfe passend gewählter Operatoren $g_1, g_2, \ldots, g_n$ G in Komplexe zerlegen (§ 24, S. 36)

$$G = H g_1 + H g_2 + \ldots + H g_n \qquad (g_1 = 1)\,, \tag{1}$$

so daß nicht zwei Summanden der rechten Seite einen Operator gemeinsam haben. Ist nun g' ein willkürlich gewählter Operator aus G, so findet sich das Produkt $g_1 g' = g'$ in einem der Summanden $H g_\alpha$, und folglich stimmen alle Operatoren $H g_1 g'$ mit denen von $H g_\alpha$ überein. Ähnliches gilt von $g_2 g', \ldots, g_n g'$, und da $H g_\alpha g' \neq H g_\beta g'$ ist, so sieht man, daß die Zerlegung

$$G = H g_1 g' + H g_2 g' + \ldots + H g_n g' \tag{1*}$$

bis auf die Anordnung der Summanden mit der früheren (1) übereinstimmt. Dabei wird durch jeden Operator g' eine Permutation der n Komplexe

$$H g_1\,,\; H g_2\,,\; \ldots,\; H g_n \tag{2}$$

hervorgerufen; diese mag mit γ' bezeichnet werden. Da zu dem Produkte $g'g''$ die Zerlegung

$$G = H g_1 g' g'' + H g_2 g' g'' + \ldots + H g_n g' g''$$

gehört, so ist der Komposition $g'g''$ die Komposition $\gamma'\gamma''$ zugeordnet, und die $\gamma', \gamma'', \ldots$ bilden eine zu G isomorphe Gruppe Γ der n Elemente (2). Γ ist transitiv; denn um $H g_\alpha$ auf $H g_\beta$ folgen zu lassen, reicht es ja aus, $g' = g_\beta^{-1} g_\alpha$ zu nehmen. Wie man sieht, ist hier die Art der Komposition von der gewöhnlich verwendeten verschieden.

Es fragt sich, welcher Teiler von G dem Einheitsoperator in Γ entspricht. Ist g_0 ein Operator dieses Teilers von G, so muß $H g_\varrho g_0$ für jedes g_ϱ zu $H g_\varrho$ werden, also $g_\varrho g_0$ zu $H g_\varrho$ gehören und g_0 zu $g_\varrho^{-1} H g_\varrho$. Folglich gehört g_0 zu der Gruppe

$$D = \} H, \; g_2^{-1} H g_2, \; g_3^{-1} H g_3, \; \ldots, \; g_n^{-1} H g_n \{ .$$

Umgekehrt liefert jedes g_0 aus D, wenn h eine Substitution aus H bedeutet, für jedes $\varrho = 2, 3, \ldots, n$

$$g_0 = g_\varrho^{-1} h g_\varrho, \quad g_\varrho g_0 = h g_\varrho, \quad H g_\varrho g_0 = H g_\varrho .$$

D ist der größte selbstkonjugierte Teiler von G, der in H enthalten ist.

Demnach wird Γ einstufig isomorph zu der Faktorgruppe G/D.

Hat die Gruppe G der Ordnung r den Teiler H der Ordnung s, und ist D der größte echt in H enthaltene selbstkonjugierte Teiler von G, so läßt sich die Faktorgruppe G/D als transitive Gruppe Γ von $r:s$ Elementen darstellen. Ist $D = 1$, so ist G als Substitutionengruppe von $r:s$ Elementen darstellbar.

§ 120. Wir bleiben bei den Bezeichnungen des vorigen Paragraphen und setzen $D = 1$ voraus. Wir untersuchen den Fall, daß es einen echten Teiler A von G gibt, der seinerseits H als echten Teiler enthält. Man sieht leicht, daß A der Komplex einer Anzahl von Summanden von (1) wird. Wir können also setzen

$$A = H g_1 + H g_2 + \ldots + H g_\varrho \qquad (g_1 = 1), \tag{3}$$

wobei ϱ ein Teiler von n ist. Gesetzt, ein g' führt eins dieser $H g_\alpha$ in ein anderes $H g_\beta$ über ($\alpha, \beta = 1, 2, \ldots, \varrho$), so daß

$$H g_\alpha g' = H g_\beta \quad \text{und} \quad g' = (H g_\alpha)^{-1} (H g_\beta)$$

wird, dann gehört also g' zur Gruppe A, und man hat

$$A = H g_1 g' + H g_2 g' + \ldots + H g_\varrho g' . \tag{3a}$$

Folglich führt jedes γ aus Γ, das einen Summanden von (3) in einen anderen von (3) umwandelt, alle aus (3) ineinander über, d. h. Γ ist eine imprimitive Gruppe.

Wenn umgekehrt Γ eine imprimitive Gruppe der Elemente (2) ist, so zerfallen diese Elemente (2) in Systeme der Imprimitivität, unter denen eins

$$(4) \qquad H g_1, H g_2, \ldots, H g_\varrho \qquad (g_1 = 1)$$

sein möge. Jede Substitution γ' der Gruppe Γ, die eins der Elemente (4) in ein anderes von (4) umwandelt, vertauscht alle aus (4) nur unter sich. Dem γ' entspreche g' in G, dann wird jedes g', für das $H g' = H g_\alpha$ ist ($\alpha = 1, 2, \ldots, \varrho$), auch $H g_\beta g' = H g_\gamma$ liefern, wobei $\beta, \gamma = 1, 2, 3, \ldots, \varrho$. Hierbei ist β willkürlich und γ durch β bestimmt. Da aus der ersten Gleichung folgt, daß g' zu $H g_\alpha$ gehört, so ergibt sich aus der zweiten

$$H g_\beta \cdot H g_\alpha = H g_\gamma, \qquad (\alpha, \beta, \gamma = 1, 2, \ldots, \varrho)$$

d. h. der Komplex der Substitutionen von G, die in den ϱ Summanden (4) vereinigt sind, bildet eine Gruppe, die H als echten Teiler enthält und gleichzeitig als echter Teiler in G enthalten ist.

Wird im Theoreme des vorigen Paragraphen $D = 1$, so ist die darstellende Gruppe Γ imprimitiv oder primitiv, je nachdem ein echter Teiler von G besteht oder nicht, der H enthält.

§ 121. Aus den Ergebnissen der beiden letzten Paragraphen läßt sich eine Reihe von Schlüssen ziehen, von denen wir einige hier anführen wollen.

I. Hat eine imprimitive Gruppe G Substitutionen, die, ohne gleich 1 zu sein, die einzelnen Imprimitivitätssysteme sämtlich ungeändert lassen, dann ist die Gruppe G zusammengesetzt, da ja diese Substitutionen mit der Einheit zusammen einen selbstkonjugierten Teiler bilden. Natürlich kann es noch andere selbstkonjugierte Teiler in der Gruppe G geben. Ist aber die Gruppe einfach, so enthält sie keine Substitutionen außer der Einheit, die kein Imprimitivitätssystem umstellen. In diesem Falle wählen wir für das H der beiden vorigen Paragraphen die Einheit $H = 1$; dann wird auch $D = 1$ und Γ einstufig isomorph zu G. Die Gruppe, deren Elemente die Imprimitivitätssysteme $S_1, S_2, \ldots$ sind, ist einstufig isomorph zu Γ; sie ist transitiv und ihr Grad ein Teiler des Grades von G. Eine imprimitive Gruppe des Grades

n ist entweder zusammengesetzt oder einer transitiven Gruppe isomorph, deren Grad ein eigentlicher Teiler von n ist.

II. Hat eine einfache Gruppe der Ordnung $r = s \cdot n$ einen Teiler der Ordnung s, so ist sie (einstufig isomorph) als transitive Gruppe des Grades n darstellbar. Denn wenn man den Teiler der Ordnung s als Gruppe H in der bisherigen Bezeichnung nimmt, findet sich $D = 1$, da ja überhaupt kein selbstkonjugierter Teiler > 1 vorhanden ist.

III. Eine einfache Gruppe kann stets (einstufig isomorph) als Substitutionengruppe in primitiver Form dargestellt werden. Dazu reicht es aus, als Gruppe H einen Maximalteiler von G zu wählen. Ein eigentlicher Maximalteiler ist nur dann nicht vorhanden, wenn die Ordnung der Gruppe eine Primzahl ist; für diesen Fall wird aber der Satz selbstverständlich.

§ 122. Die Untersuchungen der drei voraufgehenden Paragraphen haben uns auf das folgende wichtige Problem geführt: Es soll eine gegebene abstrakte Gruppe einstufig isomorph als transitive Substitutionengruppe auf alle möglichen Arten dargestellt werden. Eine Methode der Lösung ist in § 119, S. 150 gegeben; wir wollen nun zeigen, daß durch sie alle überhaupt möglichen Darstellungen der Gruppe geliefert werden.

Gegeben sei die transitive Substitutionengruppe G der Ordnung $r = n \cdot s$ und des Grades n mit den Elementen $x_1, x_2, \ldots, x_n$. Es sei H der Teiler von G, der x_1 nicht umsetzt, dann enthält der Komplex $H g_\alpha$ alle und nur die Substitutionen von G, die auf x_1 folgen lassen x_α, falls g_α eine beliebige von ihnen ist. Man hat

$$G = H + H g_2 + H g_3 + \ldots + H g_n .$$

Wir betrachten nun wieder die Komplexe

$$H, H g_2, H g_3, \ldots, H g_n$$

als n Operatoren; dann zeigen die Schlüsse aus § 119, daß diese als Elemente einer zu G isomorphen Substitutionengruppe Γ gedeutet werden können. Ferner sieht man, daß die dort mit D bezeichnete Gruppe, nämlich

$$D = \} H, g_2^{-1} H g_2, \ldots, g_r^{-1} H g_r \{ ,$$

hier den Wert 1 hat. Denn da H das Element x_1 nicht umstellt, so kommen in der Klammer Transformierte vor, die $x_2, x_3, \ldots, x_n$ nicht umstellen. D kann also als selbstkonjugierter Teiler nur die Einheit enthalten, und Γ ist zu G einstufig isomorph.

Ist nun eine abstrakte Gruppe G' der Ordnung $r = n \cdot s$ als transitive Substitutionengruppe G von n Elementen darstellbar, dann hat G einen Teiler der Ordnung $s = r : n$, derart, daß der selbstkonjugierte Maximalteiler der Gruppe $r$ter Ordnung, der als Teiler H der Gruppe $s$ter Ordnung auftritt, zur Einheit wird. Wenn nun die abstrakte Gruppe G' einstufig isomorph zur transitiven Substitutionengruppe G ist, dann reicht es aus, in § 119 für den Teiler H' von G' den zu wählen, der dem H in G isomorph ist, um zu G zurück zu gelangen.

Es ist hiernach das Problem der Darstellung von G darauf zurückgeführt, alle Teiler H' von G' zu bestimmen.

Wir wollen als Beispiel die alternierende Gruppe G' von 5 Elementen und der Ordnung 60 behandeln und als transitive Gruppe auf alle möglichen Arten darzustellen suchen; dabei kommt es also auf die Bestimmung aller Teiler H' von G' an. Diese können als Ordnungszahlen nur haben

$$2, 3, 4, 5, 6, 10, 12, 15, 20, 30;$$

die Grade der Teiler H' werden bzw.

$$30, 20, 15, 12, 10, 6, 5, 4, 3, 2.$$

Die drei letzten Möglichkeiten müssen ausgeschaltet werden, da aus vier, oder drei, oder zwei Elementen keine Gruppe der Ordnung 60 gebildet werden kann. Die sieben ersten Möglichkeiten verwirklichen sich auf je eine Art, nämlich durch die folgenden Teiler H'

$$s = 2; \quad H' = \{(x_1 x_2)(x_3 x_4)\};$$
$$s = 3; \quad H' = \{(x_1 x_2 x_3)\};$$
$$s = 4; \quad H' = \{(x_1 x_2)(x_3 x_4), (x_1 x_3)(x_2 x_4)\};$$
$$s = 5; \quad H' = \{(x_1 x_2 x_3 x_4 x_5)\};$$
$$s = 6; \quad H' = \{(x_1 x_2 x_3), (x_1 x_2)(x_4 x_5)\};$$
$$s = 10; \quad H' = \{(x_1 x_2 x_3 x_4 x_5), (x_2 x_5)(x_3 x_4)\};$$
$$s = 12; \quad H' = \{(x_1 x_2 x_3), (x_1 x_2)(x_3 x_4)\}.$$

Bei diesen Bildungen ist darauf zu achten, daß die konstituierenden Substitutionen sämtlich gerade sind. In allen Fällen ist $D' = 1$, wie aus der Bemerkung folgt, daß nach § 64, S. 81 die alternierende Gruppe einfach ist.

§ 123. Zum Schlusse dieses Kapitels wollen wir noch die primitiven Gruppen der niedrigsten Grade zusammenstellen.

I. Es sei $n = 2$ der Grad der primitiven Substitutionengruppe G. Offenbar ist

$$G = [1\,,\ (x_1\, x_2)]\,.$$

II. Für $n = 3$ findet man zwei Gruppen, die primitiv sind,

$$G_1 = \{(x_1\, x_2\, x_3)\,,\ (x_1\, x_2)\}\,, \quad G_2 = \{(x_1\, x_2\, x_3)\}\,,$$

die symmetrische und die alternierende Gruppe.

III. Wir nehmen $n = 4$. Dann wird die Ordnung der Gruppe G ein Teiler von $4! = 24$ und wegen der Transitivität ein Vielfaches von 4, also eine der Zahlen 4, 8, 12, 24. Die beiden letzten Zahlen führen auf die alternierende und auf die symmetrische Gruppe, die beide primitiv sind.

Die Gruppen von der Ordnung 4 haben wir in § 16, S. 24 behandelt. Es sind die zyklische Gruppe

$$G = \{(x_1\, x_2\, x_3\, x_4)\}$$

und die Vierergruppe

$$G = \{(x_1\, x_2)\,(x_3\, x_4)\,,\ (x_1\, x_3)\,(x_2\, x_4)\}\,;$$

beide sind imprimitiv.

Die Gruppen von der Ordnung 8 sind in § 71, S. 91 aufgestellt worden. Von den dort gefundenen Abelschen können wir absehen, denn nach § 108, S. 141 sind es reguläre Gruppen, und deshalb sind sie nach § 116, S. 147 imprimitiv. Weiter erhält man außer diesen noch

$$G_1' = \{(1234)\,(5678)\,,\ (15)\,(28)\,(37)\,(46)\}$$

und

$$G_2' = \{(1234)\,(5678)\,,\ (1537)\,(2846)\}\,.$$

Bei der Untersuchung, ob eine Gruppe primitiv oder imprimitiv sei, reicht es aus, die konstituierenden Sub-

stitutionen in Betracht zu ziehen. Dabei liefert nun G_1' sofort die beiden Imprimitivitätssysteme

$$1, 3, 5, 7, \quad \text{und} \quad 2, 4, 6, 8 .$$

G_1' ist also imprimitiv.

Bei G_2' ist genau das gleiche der Fall. Auch hier treten dieselben beiden Systeme auf.

Es bleiben somit als primitive Gruppen des Grades 4 wieder nur die symmetrische und die alternierende zurück.

IV. Endlich behandeln wir noch $n = 5$. Hier ist, wie bei jedem Primzahlgrade, jede transitive Gruppe primitiv. Es kommt also nur auf die Bestimmung dieser transitiven Gruppen von fünf Elementen an. Ihre Ordnungen können nur

$$5, 10, 15, 20, 30, 40, 60, 120$$

sein. Die alternierende sowie die symmetrische Gruppe der fünf Elemente x_1, x_2, x_3, x_4, x_5 gehören zu den gesuchten Gruppen.

Keine der übrigen, etwa noch vorhandenen, kann eine Substitution von einer der Formen

$$(x_1 x_2) \quad \text{oder} \quad (x_1 x_2 x_3) \quad \text{oder} \quad (x_1 x_2)(x_3 x_4 x_5)$$

enthalten, weil die Gruppe sonst alternierend oder symmetrisch wäre (§ 117, S. 148). Also können nur Substitutionen von einer der Formen

$$(x_1 x_2)(x_3 x_4) \quad \text{oder} \quad (x_1 x_2 x_3 x_4) \quad \text{oder} \quad (x_1 x_2 x_3 x_4 x_5)$$

vorkommen. Da die Gruppe transitiv ist, muß sie Substitutionen enthalten, die alle fünf Elemente umsetzen (§ 101, S. 130), also von der Form sind $s_0 = (x_1 x_2 x_3 x_4 x_5)$. Ferner ist, da kein $(x_1 x_2 x_3)$ vorkommt, die Ordnung der Gruppe r nicht durch 3 teilbar, also r ein Teiler von 40. Nun wird nach dem III. Sylowschen Satze (§ 81, S. 104)

$$r = 5 \cdot m(1 + 5 \cdot k) ,$$

und $m(1 + 5 \cdot k)$ ist ein Teiler von 8; daher $k = 0$, und $\{s_0\}$ ein selbstkonjugierter Teiler der Gruppe. Sucht man nun nach § 32, S. 48 alle Substitutionen von x_2, x_3, x_4, x_5, die $\{s_0\}$ in sich transformieren, so findet man nur die drei

$$(x_2 x_3 x_5 x_4), \ (x_2 x_5)(x_3 x_4), \ (x_2 x_4 x_5 x_3) .$$

Daher kommt allein eine der beiden metazyklischen Gruppen

$$G_1 = \{(x_1\,x_2\,x_3\,x_4\,x_5)\,,\ (x_2\,x_3\,x_5\,x_4)\}\,,$$
$$G_2 = \{(x_1\,x_2\,x_3\,x_4\,x_5)\,,\ (x_2\,x_5)\,(x_3\,x_4)\}$$

in Frage, deren zweite ein Teiler der ersten ist.

Für $n = 5$ gibt es also vier primitive Gruppen: die alternierende, die symmetrische, die Gruppe G_1 von der Ordnung 20 und die Gruppe G_2 von der Ordnung 10.

---

11. Kapitel.

Substitutionengruppen. — Gruppen höchster Ordnungen bei gegebenem Grade.

§ 124. Sind n Elemente $x_1, x_2, \ldots, x_n$ gegeben, so ist die Gruppe höchster Ordnung, die sich aus ihnen bilden läßt, die symmetrische, und ihre Ordnung ist $r = n!$ Die Gruppe der nächst kleineren Ordnung ist die alternierende mit $r = \frac{1}{2}\,n!$, d. h. mit dem Index 2 gegen die symmetrische. In § 26, S. 40 ist bewiesen worden, daß die alternierende Gruppe auch die einzige dieser Ordnung oder dieses Index ist. Ferner können wir die symmetrische Gruppe der $(n-1)$ Elemente $x_1, x_2, \ldots, x_{n-1}$ als Teiler der von $x_1, x_2, \ldots, x_n$ ansehen und kommen so auf eine Gruppe $n$ten Grades von der Ordnung $(n-1)!$ und mit dem Index n gegen die symmetrische Gruppe von n Elementen. Wir werfen die Frage auf, ob es Gruppen $n$ten Grades gibt, deren Ordnung zwischen $\frac{1}{2}\,n!$ und $(n-1)!$ liegt, so daß der zugehörige Index, der im folgenden stets auf die symmetrische Gruppe bezogen werden soll, falls nichts anderes bestimmt wird, zwischen 2 und n fällt.

Gesetzt, wir haben eine solche Gruppe G, so denken wir uns alle ihre r Substitutionen in Form von Zyklenkomplexen hingeschrieben. Aus allen diesen denken wir uns weiter ein Element, etwa x_1, weggewischt, dann bleiben Zyklen von $(n-1)$ Elementen zurück, die wir wieder als Substitutionen deuten. Diese werden im allgemeinen keine Gruppe, sondern nur einen Komplex K bilden. Die Anzahl der so erhaltenen Substitutionen ist $r > (n-1)!$ Nun gibt es aber nur $(n-1)!$ verschiedene Substitutionen von

$(n-1)$ Elementen; folglich enthält K mindestens zwei gleiche Substitutionen. Es müssen daher in G verschiedene Substitutionen vorkommen, die in K identisch werden, die sich also in G nur durch die Stellung des einen Elementes x_1 unterscheiden. Das kann auf zweierlei Art geschehen, entweder so, wie bei den Substitutionen

$$s_1 = \ldots x_\varkappa x_1 x_\lambda \ldots x_\mu x_\nu \ldots \text{ und } s_2 = \ldots x_\varkappa x_\lambda \ldots x_\mu x_1 x_\nu \ldots,$$

wobei in der Bezeichnung nur die Verschiedenheit hervorgehoben ist; oder so, wie bei

$$t_1 = \ldots x_\varkappa x_1 x_\lambda \ldots \quad \text{und} \quad t_2 = \ldots x_\varkappa x_\lambda \ldots (x_1) .$$

Demnach kommt in der Gruppe G auch vor entweder die Zirkularsubstitution

$$s_1 \cdot s_2^{-1} = (x_\varkappa x_\mu x_1) ,$$

oder die Transposition

$$t_1 t_2^{-1} = (x_\varkappa x_1) .$$

Nun muß G aber transitiv und für $n > 4$ auch primitiv sein. Denn wäre G intransitiv, so würde es nach § 106, S. 139 als Maximum der Ordnung $(n-1)!$ haben, während doch $r > (n-1)!$ angenommen war; und wäre G zwar transitiv, aber imprimitiv, so würde nach § 113, S. 145 als Maximum der Ordnung $r = 2!\left(\frac{n}{2}!\right)^2$ für $n > 4$ kleiner als $(n-1)!$ werden. Für $n > 4$ ist also G primitiv; nach § 117, S. 148 wird dann G alternierend oder symmetrisch.

Für $n = 4$ ist dagegen $2(2!)^2 = 8 > 3!$. Hier kann demnach eine Gruppe der verlangten Eigenschaft erscheinen. Wir sind einer solchen schon mehrfach begegnet; sie tritt in der Form auf

$$1 , \ (x_1 x_2) , \ (x_3 x_4) , \ (x_1 x_2)(x_3 x_4) , \ (x_1 x_3)(x_2 x_4) , \ (x_1 x_4)(x_2 x_3)$$
$$(x_1 x_3 x_2 x_4) , \ (x_1 x_4 x_2 x_3) ;$$

für sie ist der Index 3 wirklich größer als 2 und kleiner als der Grad $n = 4$. Dies ist der einzige Typus von Gruppen mit $r = 2 \cdot 4$ und $n = 4$, wie aus dem zweiten Sylowschen Satze § 80, S. 103 folgt, wenn man $p = 2$ und $\alpha = 3$ setzt; denn alle vorhandenen bilden ein einziges konjugiertes System.

Eine Gruppe des Grades n, deren Ordnung größer als $(n-1)!$ ist, wird alternierend oder symmetrisch, falls $n > 4$ ist. Für $n = 4$ dagegen bildet die Gruppe

$$G = \{(x_1 x_2), (x_1 x_3)(x_2 x_4)\}$$

eine Ausnahme; ihre Ordnung ist gleich 8.

§ 125. Wir gehen zur Untersuchung der Gruppe G des Index n, also der Ordnung $r = (n-1)!$ beim Grade n und den Elementen $x_1, x_2, \ldots, x_n$ über. Denken wir uns auch hier die Substitutionen in Zyklen hingeschrieben und dann ein Element, etwa x_1, in allen getilgt, so bleiben $(n-1)!$ Substitutionen eines Komplexes K der $(n-1)$ Elemente $x_2, x_3, \ldots, x_n$ zurück. Unter den Substitutionen von K kann es gleiche geben; es können aber auch alle untereinander verschieden sein. Im ersten Falle kommen wir auf die Betrachtungen des vorigen Paragraphen zurück und sehen, daß G ein $(x_\varkappa x_\mu x_1)$ oder ein $(x_\varkappa x_1)$ enthält. Wäre G transitiv und primitiv, so fiele es wegen der Existenz dieser Substitutionen mit der alternierenden oder mit der symmetrischen Gruppe des Grades n zusammen. Wäre G transitiv und imprimitiv, so wäre seine Ordnung höchstens $2\left(\frac{n}{2}!\right)^2 < (n-1)!$ für $n > 4$. Es kann also G nur intransitiv sein und muß dabei den Maximalwert $(n-1)!$ der Ordnung annehmen. Dann fällt G mit der symmetrischen Gruppe von $(n-1)$ Elementen zusammen.

Im zweiten Falle, daß es unter dem, aus G durch Unterdrückung von x_1 hervorgehenden Substitutionenkomplexe K keine gleichen Substitutionen gibt, bilden diese zusammen alle der Elemente $x_2, x_3, \ldots, x_n$. Also kommen insbesondere alle Transpositionen von $x_2, x_3, \ldots, x_n$, nämlich

(1) $$(x_2 x_3), (x_2 x_4), (x_3 x_4), \ldots, (x_{n-1} x_n),$$

vor. Wäre nun in G das Element x_1 mit keinem anderen Elemente transitiv verbunden, so würden die Transpositionen (1) unverändert auch in G vorkommen, und wir würden wieder auf den eben besprochenen Fall stoßen,

daß G symmetrisch in $(n-1)$ Elementen ist; denn (1) liefert ja diese symmetrische Gruppe.

Wir nehmen also an, x_1 sei mit einem der übrigen Elemente verbunden und deshalb mit allen. G ist dann transitiv. Wir setzen ferner voraus $n \geqq 7$.

Käme in G eine Transposition (1) vor, so wäre G bei Primitivität von zu hoher Ordnung, bei Nichtprimitivität von zu niedriger. Also muß in G entweder ein

$$(x_1 x_2 x_3) \quad \text{oder ein} \quad (x_1 x_4)(x_2 x_3)$$

auftreten. Von der ersten Möglichkeit müssen wir aus gleichen Gründen absehen, die das Erscheinen einer Transposition ausschlossen. Es bleibt daher nur die Möglichkeit

(2) $$(x_1 x_4)(x_2 x_3) = t$$

zurück. Diesen Fall haben wir zu untersuchen.

In dem Komplexe, der nach Unterdrückung von x_1 aus G entsteht, kommt ein

$$\sigma = (x_3 x_5 x_6 x_7 x_4)$$

vor, also in G je nach der ursprünglichen Stellung des x_1 eine der sieben Substitutionen $\sigma, \sigma_1, \ldots, \sigma_6$, die hier folgen:

$$\sigma = (x_3 x_5 x_6 x_7 x_4), \qquad \sigma_1 = (x_1 x_\alpha)(x_3 x_5 x_6 x_7 x_4),$$
$$\sigma_2 = (x_1 x_3 x_5 x_6 x_7 x_4), \quad \sigma_3 = (x_1 x_5 x_6 x_7 x_4 x_3),$$
$$\sigma_4 = (x_1 x_6 x_7 x_4 x_3 x_5), \quad \sigma_5 = (x_1 x_7 x_4 x_3 x_5 x_6),$$
$$\sigma_6 = (x_1 x_4 x_3 x_5 x_6 x_7).$$

Alle diese sieben Fälle sind unmöglich, wie sich leicht zeigt. Denn

I. σ und t liefern

$$([t\sigma]^3 \sigma)^2 = (x_3 x_5 x_7).$$

II. σ_1 liefert

$$\sigma_1^5 = (x_1 x_\alpha).$$

III. σ_2 und t liefern

$$(\sigma_2^3 t)^4 = (x_2 x_3 x_7).$$

IV. σ_3 und t liefern

$$(\sigma_3^3 t)^4 = (x_2 x_3 x_6).$$

V. σ_4 und t liefern

$$(\sigma_4^3 t)^3 = (x_5 x_7) .$$

VI. σ_5 und t liefern

$$(\sigma_5^3 t)^5 = (x_5 x_7) .$$

VII. σ_6 und t liefern

$$(\sigma_6^3 t)^4 = (x_2 x_3 x_7) .$$

In all diesen Fällen stößt man also, wie man sieht, auf Substitutionen, die die alternierende oder die symmetrische Gruppe hervorrufen, wenn G primitiv ist. Und ein imprimitives G hat zu geringe Ordnung. Demnach gibt es für $n \geqq 7$ keine Gruppe mit dem Index n außer der symmetrischen von $(n-1)$ Elementen.

Aber auch für $n = 5$ ist keine andere Gruppe vorhanden. Hier würde nämlich die Ordnung von G gleich $4!$ sein. In unserem Systeme K käme $\tau = (x_2 x_5 x_3 x_4)$ vor. Das fehlende Element x_1 kann nicht in den Zyklus von τ treten, denn G enthielte sonst eine Substitution fünfter Ordnung und es wäre die Ordnung von G durch 5 teilbar. τ selbst käme daher in G vor; damit aber auch die Potenz

$$(t \tau)^3 = (x_3 x_5) .$$

Ebensowenig ist es bei $n = 3$ oder 4 möglich, solche Ausnahmegruppen zu bilden.

Ist die Ordnung einer Gruppe $n$ten Grades gleich $(n-1)!$, so ist es bei $n \neq 6$ die symmetrische Gruppe von $(n-1)$ Elementen.

§ 126. Wir wollen nun dem Falle $n = 6$ näher treten und die transitiven Gruppen des Grades 6 und der Ordnung 120 aufsuchen.

In dem Komplexe K, der durch die Unterdrückung von x_1 in den Substitutionen von G entsteht, und der mit der symmetrischen Gruppe der fünf Elemente x_2, x_3, x_4, x_5, x_6 identisch ist, kommen die zehn Transpositionen vor, deren Indizes die folgenden sind:

(3) (23), (24), (25), (26), (34), (35), (36), (45), (46), (56) .

In G tritt nach dem vorigen Paragraphen zu jeder dieser

Transpositionen ein $(x_1 x_\alpha)$ hinzu, so daß in G zehn Substitutionen enthalten sind, die die Form haben

(4) $\quad (1\,a)\,(23)\,,\ (1\,b)\,(24)\,,\ (1\,c)\,(25)\,,\ \ldots,\ (1\,g)\,(56)\,,$

wo $a, b, c, \ldots, g$ nur $2, 3, 4, 5, 6$ sein können. Es muß also einer der Indizes $a, b, c, \ldots$ mehrfach in (4) auftreten. Da die Bezeichnung in unserem Belieben steht, sei dies der Index 4 in $(14)\,(23)$. Ein zweites (14) kann nur mit einer der fünf Transpositionen aus (3)

$$(25)\,,\ (26)\,,\ (35)\,,\ (36)\,,\ (56)$$

verbunden sein, d. h. es muß von den fünf Substitutionen

$$(14)\,(25)\,,\ (14)\,(26)\,,\ (14)\,(35)\,,\ (14)\,(36)\,,\ (14)\,(56)$$

eine zu G gehören. Die vier ersten sind es nicht, wie die Multiplikation mit dem, der Annahme nach vorhandenen $(14)\,(23)$ zeigt; denn sonst enthielte G eine Zirkularsubstitution dritter Ordnung, was nach dem ersten Absatze von § 125 nicht möglich ist. Also gibt es in G die beiden Substitutionen

(5) $\quad (14)\,(23) \quad \text{und} \quad (14)\,(56)\,.$

In dem Komplexe K, der durch die Unterdrückung von x_1 entsteht, kommt auch (234) vor, folglich in G eine der Substitutionen

$$(234)\,,\ (15)\,(234)\,,\ (16)\,(234)\,,\ (1234)\,,\ (1342)\,,\ (1423)\,.$$

Es zeigt sich sofort die Unmöglichkeit der zweiten und dritten Annahme; die der ersten, vierten und sechsten folgt durch Multiplikation mit $(14)\,(23)$. Also enthält G

(6) $\quad s = (1342) \quad \text{und ebenso} \quad \sigma = (1546)\,,$

wie sich zeigt, wenn man von $(14)\,(56)$ statt von $(14)\,(23)$ in (5) Gebrauch macht.

Ähnliche Schlüsse beweisen für G die Existenz einer der sechs Substitutionen

$$(2354)\,,\ (16)\,(2354)\,,\ (12354)\,,\ (13542)\,,\ (15423)\,,\ (14235)\,,$$

die aus dem Auftreten von (2354) in K folgt.

Aber die zweite, dritte, vierte und sechste können nicht vorkommen wegen der sonst in G bzw. vorhandenen

$$((16)(2354))^2 \cdot (14)(56) \cdot (16)(2354) \cdot (14)(56) \cdot (16)(2354) = (134);$$
$$(12354) \cdot (14)(23) = (135);$$
$$(14)(23) \cdot (13542)^{-1} \cdot (14)(23) \cdot (13542) = (145);$$
$$(14)(23) \cdot (14235) = (125).$$

Andererseits liefern die erste und die fünfte das gleiche, wenn man von der, wegen der Konstitution von (5) und (6) erlaubten Vertauschung der Indizes 2 und 3 absieht. Denn es ist ja

$$((14)(23) \cdot (2354)^2)^2 = (15432),$$

und umgekehrt findet man

$$(1342) \cdot (15423) = (3254),$$

so daß jede der beiden Möglichkeiten — die Annahme von (2354) oder von (15423) — aus der anderen folgt. Also reicht es aus, für G die Existenz anzunehmen von

$$t = (15423).$$

Nun ist $s\,t = t^3 s$, d. h. $\{s\}$ ist mit $\{t\}$ vertauschbar. G enthält somit den Teiler

$$H = \{s, t\}$$

der Ordnung $4 \cdot 5 = 20$. Jede Substitution von H kann auf eine der Formen gebracht werden

$$s^\alpha t^\beta \quad \text{oder} \quad t^\gamma s^\delta$$
$$(\alpha, \delta = 0, 1, 2, 3; \beta, \gamma = 0, 1, 2, 3, 4).$$

Ferner enthält G das Produkt

$$u = \sigma t = (146523),$$

für das die Relationen gelten

$$u\,t = t^4 u^5, \quad u\,s = s^3 t^3 u,$$

mit deren Hilfe alle Substitutionen von $\{s, t, u\}$ auf die Form

$$s^\alpha t^\beta u^\varepsilon$$
$$(\alpha = 0, 1, 2, 3; \quad \beta = 0, 1, 2, 3, 4; \quad \varepsilon = 0, 1, \ldots, 5)$$

gebracht werden können. Alle diese 120 Substitutionen sind voneinander verschieden. Denn aus einer Gleichung

$$s^\alpha t^\beta u^\varepsilon = s^{\alpha'} t^{\beta'} u^{\varepsilon'}$$

folgt, daß $u^{\varepsilon-\varepsilon'}$ zu H gehört; also muß $\varepsilon = \varepsilon'$ sein, da H das Element 6 nicht umsetzt; usf.

Demnach ist schließlich

$$G = \{s, t, u\}.$$

Es gibt eine transitive Gruppe 6ten Grades vom Index 6, also von der Ordnung 120, nämlich

$$G = \{(x_1 x_3 x_4 x_2), (x_1 x_5 x_4 x_2 x_3), (x_1 x_4 x_6 x_5 x_2 x_3)\}.$$

Außerdem gibt es noch eine intransitive Gruppe 6ten Grades vom Index 6, die mit der symmetrischen Gruppe von fünf Elementen identisch ist.

§ 127. Wir wollen nun weiter annehmen, eine Gruppe G des Grades n habe die Ordnung r, und es sei

$$r > (n-k)!.$$

Unterdrückt man in allen Substitutionen von G die k Elemente $x_1, x_2, x_3, \ldots, x_k$, so erhält man einen Komplex von Substitutionen aus $(n-k)$ Elementen, der mehr als $(n-k)!$ Substitutionen dieser Elemente enthält. Dies ist wegen der Anzahl der verschiedenen Substitutionen von $(n-k)$ Elementen nur möglich, wenn der Komplex gleiche Substitutionen enthält, so daß unter den Substitutionen von G solche vorkommen, die sich nur durch die Stellung der $x_1, x_2, \ldots, x_k$ voneinander unterscheiden. s_1 und s_2 seien zwei solche; dann kann das Produkt $s_1 \cdot s_2^{-1}$ außer den Elementen $x_1, x_2, \ldots, x_k$ nur Elemente enthalten, die in s_1 oder in s_2 einem der Elemente $x_1, x_2, \ldots, x_k$ vorausgehen. Denn gehört x_α nicht zu diesen, so enthält s_1 wie s_2 dieselbe Folge $x_\alpha x_\beta$ und in $s_1 s_2^{-1}$ fällt x_α fort. Es kommen daher in G Substitutionen von nicht mehr als $3k$ Elementen vor. Nun müssen die Substitutionen einer Gruppe, die möglichst wenige Elemente umsetzen, regulär sein, da sonst eine ihrer Potenzen, ohne gleich 1 zu werden, weniger Elemente enthielte als sie selber. Wir haben demnach den Satz: Ist die Ordnung r einer Gruppe $n$ten Grades $>(n-k)!$, so enthält sie reguläre Substitutionen von höchstens $3k$ Elementen.

Die weitere Untersuchung müßte daher an den Begriff der Klasse einer Substitutionengruppe anknüpfen (§ 100, S 128).

---

12. Kapitel.

Analytische Darstellung der Substitutionen. Die lineare Gruppe.

§ 128. Wir sind gelegentlich, § 103, S. 132, auf die analytische Darstellung von Substitutionen gekommen; hier wollen wir uns mit einer genaueren Untersuchung der dabei auftretenden Verhältnisse beschäftigen. Die Elemente $x_1, x_2, x_3, \ldots, x_n$ der Substitutionen sollen durch die Angabe ihrer Indizes bezeichnet werden, also x_i einfach durch i. Dann kann man die Substitution

$$s_i = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix} = \begin{pmatrix} \alpha \\ i_\alpha \end{pmatrix} = |\alpha, i_\alpha|$$

darstellen durch

$$s_i = |\alpha, \varphi(\alpha)|, \quad \text{oder noch kürzer durch} \quad s_i = |\varphi(\alpha)|,$$

wo φ eine Funktion von α ist, die nur die Bedingungen zu erfüllen hat

$$\varphi(1) = i_1, \ \varphi(2) = i_2, \ \varphi(3) = i_3, \ \ldots, \ \varphi(n) = i_n .$$

Dies kann auf unendlich viele Arten geschehen; beispielsweise mit Hilfe der Lagrangeschen Interpolationsformel, indem man zuerst

$$f(\alpha) = (\alpha - 1)(\alpha - 2)(\alpha - 3) \ldots (\alpha - n); \quad f'(\alpha) = \frac{df(\alpha)}{d\alpha}$$

und dann

$$\varphi(\alpha) = i_1 \frac{f(\alpha)}{(\alpha - 1) f'(1)} + i_2 \frac{f(\alpha)}{(\alpha - 2) f'(2)} + \ldots + i_n \frac{f(\alpha)}{(\alpha - n) f'(n)}$$

setzt. Daß nicht jede numerische Funktion von α zur Darstellung einer Substitution benutzt werden kann, folgt einfach daraus, daß sie für $\alpha = 1, 2, 3, \ldots, n$ lauter voneinander verschiedene Werte derselben Reihe $1, 2, 3, \ldots, n$ liefern muß.

Bezeichnet n den Grad der Substitution, und ist n auf irgend eine Art in Faktoren zerlegt $n = n_1 \cdot n_2 \ldots n_\varkappa$, dann kann man die n Elemente der Substitution oder

genauer ihre Indizes durch ein System von $\varkappa$ Größen bezeichnen, etwa durch

$$x_{i_1, i_2, i_3, \ldots, i_\varkappa} \qquad (i_\alpha = 1, 2, \ldots, n_\alpha; \quad \alpha = 1, 2, \ldots, \varkappa),$$

was wir einfacher durch das Symbol

(2) $$|i_1, i_2, \ldots, i_\varkappa|$$

angeben. Die Substitution selbst wird dann durch den Übergang des Indizeskomplexes (2) in den neuen

(2a) $$|\varphi_1(i_1), \varphi_2(i_2), \ldots, \varphi_\varkappa(i_\varkappa)|$$

bestimmt. Jede der Funktionen φ_α muß dabei die Werte $1, 2, \ldots, n_\alpha$ annehmen. Offenbar sind die φ_α der Beschränkung unterworfen, daß, wenn die Argumente (2) alle ihre $n_1 \cdot n_2 \ldots n_\varkappa$ Wertkombinationen durchlaufen, das gleiche mit den Funktionalwerten (2a) der Fall ist.

Es ist übrigens nicht nötig, die Werte der φ_α auf die Werte $1, 2, \ldots, n_\alpha$ zu beschränken. Wir brauchen nur statt der Werte φ_α selbst ihre kleinsten positiven Reste modulo n_α zu setzen, also die ihnen kongruenten Zahlen der Reihe $1, 2, \ldots, n_\alpha$.

§ 129. Die einfachste Form der besprochenen Darstellung erlangen wir durch die Annahme, daß die

$$n_1 = n_2 = \ldots = n_\varkappa$$

einer Primzahl p gleich werden, und daß

$$\varphi_\alpha(i_\varrho) = i_\varrho + c_\alpha$$

wird, wobei c_α eine positive, ganzzahlige Konstante bedeutet. Dabei geht dann (2a) in die Form über

(3) $$s(c) \equiv |i_1 + c_1, i_2 + c_2, \ldots, i_\varkappa + c_\varkappa| \pmod{p}.$$

Die Anzahl derart möglicher Substitutionen ist $p^\varkappa$, da man jedem c die Werte $1, 2, \ldots, p$ oder auch $0, 1, 2, \ldots, p-1$ geben kann. Es ist ersichtlich

$$s(c) \cdot s(d) = s(c+d) = s(d) \cdot s(c);$$

also bilden die Substitutionen (3) eine Abelsche Gruppe A der Ordnung $p^\varkappa$ und des Grades $p^\varkappa$; sie heißt die arithmetische Gruppe (Cauchy).

A ist transitiv; denn das Indexsystem $a_1, a_2, \ldots, a_\varkappa$ wird in $b_1, b_2, \ldots, b_\varkappa$ durch die Substitution

$$s(b-a) = |i_1 + b_1 - a_1, \ldots, i_\varkappa + b_\varkappa - a_\varkappa|$$

übergeführt. Da es nur eine solche überführende Substitution gibt, so ist die Gruppe A einfach transitiv.

Die einfachsten Substitutionen von A sind die, bei denen nur je ein Index um eine Einheit erhöht wird:

$$|i_1+1, i_2, i_3, \ldots| = s_1, \quad |i_1, i_2+1, i_3, \ldots| = s_2,$$
$$|i_1, i_2, i_3+1, \ldots| = s_3, \quad \ldots$$

Jede andere Substitution $s(c)$ ist aus diesen $\varkappa$ voneinander unabhängigen darstellbar in der Form

$$(4) \qquad s(c) = s_1^{c_1} s_2^{c_2} \ldots s_\varkappa^{c_\varkappa}.$$

Die Abelsche Gruppe A hat daher den Rang $\varkappa$, und man hat

$$A = \{s_1, s_2, \ldots, s_\varkappa\}.$$

Nach § 108, S. 141 ist A eine reguläre Gruppe.

§ 130. Wir suchen jetzt die allgemeinste Gruppe der Substitutionen

$$t = |\varphi_1(i_1, i_2, \ldots, i_\varkappa), \varphi_2(i_1, i_2, \ldots, i_\varkappa), \ldots$$
$$\ldots, \varphi_\varkappa(i_1, i_2, \ldots, i_\varkappa)|,$$

die mit A vertauschbar sind, für die also $t^{-1} \cdot s(c) \cdot t^{+1} = s(d)$ wird. Dazu reicht es aus, für $s(c)$ der Reihe nach $s_1, s_2, s_3, \ldots, s_\varkappa$ zu nehmen. Man erhält, da t^{-1} den Index φ_α in i_α verwandelt, s_1 das i_1 in i_1+1 überführt, und t das i_1+1 in $\varphi_\alpha(i_1+1, i_2, \ldots)$ umändert,

$$t^{-1} s_1 t = \begin{pmatrix} \varphi_\alpha(i_1, i_2, i_3, \ldots, i_\varkappa) \\ \varphi_\alpha(i_1+1, i_2, i_3, \ldots, i_\varkappa) \end{pmatrix}.$$

Soll dies zur Gruppe A gehören, so muß

$$(5) \qquad \varphi_\alpha(i_1+1, i_2, \ldots, i_\varkappa) = \varphi_\alpha(i_1, i_2, \ldots, i_\varkappa) + c_{\alpha 1}$$
$$(\alpha = 1, 2, \ldots, \varkappa)$$

sein. Genau auf entsprechende Art erhält man

$$(5a) \qquad \begin{cases} \varphi_\alpha(i_1, i_2+1, \ldots, i_\varkappa) = \varphi_\alpha(i_1, i_2, \ldots, i_\varkappa) + c_{\alpha 2} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \varphi_\alpha(i_1, i_2, \ldots, i_\varkappa+1) = \varphi_\alpha(i_1, i_2, \ldots, i_\varkappa) + c_{\alpha \varkappa}. \end{cases}$$

Aus (5) schließt man durch wiederholte Anwendung derselben Reduktion

$$\varphi_\alpha(i_1+1, i_2, \ldots, i_\varkappa) = \varphi_\alpha(i_1-1, i_2, \ldots, i_\varkappa) + 2c_{\alpha 1}$$
$$= \varphi_\alpha(i_1-2, i_2, \ldots, i_\varkappa) + 3c_{\alpha 1} = \ldots,$$
$$\varphi_\alpha(i_1, i_2, \ldots, i_\varkappa) = \varphi_\alpha(0, i_2, \ldots, i_\varkappa) + c_{\alpha 1} i_1;$$

und weiter aus (5a) ebenso

$$\varphi_\alpha(i_1, i_2, \ldots, i_\varkappa) = \varphi_\alpha(0, 0, i_3, \ldots, i_\varkappa) + c_{\alpha 1} i_1 + c_{\alpha 2} i_2 .$$

Allgemein ergibt sich das Resultat

$$\varphi_\alpha(i_1, i_2, \ldots, i_\varkappa) = \varphi_\alpha(0, 0, \ldots, 0) + c_{\alpha 1} i_1 + c_{\alpha 2} i_2 + \ldots + c_{\alpha\varkappa} i_\varkappa .$$

Das Glied $\varphi_\alpha(0, 0, \ldots, 0)$ ist eine Konstante, die c_α heißen mag. Man hat dann

(6) $$\varphi_\alpha(i_1, i_2, \ldots, i_\varkappa) = c_{\alpha 1} i_1 + c_{\alpha 2} i_2 + \ldots + c_{\alpha\varkappa} i_\varkappa + c_\alpha ,$$

(7) $$\begin{cases} t = \left| \Sigma c_{1\beta} i_\beta + c_1, \Sigma c_{2\beta} i_\beta + c_2, \ldots, \Sigma c_{\varkappa\beta} i_\beta + c_\varkappa \right| \\ \qquad (\beta = 1, 2, \ldots, \varkappa). \end{cases}$$

Daß umgekehrt für jedes so gebildete t die Transformationsformel

$$t^{-1} A t = A$$

gilt, ist leicht zu sehen.

Wir untersuchen nun, welchen Bedingungen die $c_{\alpha\beta}$ unterworfen werden müssen, damit t eine Substitution darstellt. Dazu reicht es aus, daß für modulo p inkongruente Systeme der $i_1, i_2, \ldots, i_\varkappa$ die Elemente von t auch inkongruent seien; daß also die Kongruenzen mod p

$$c_{\alpha 1} i_1 + c_{\alpha 2} i_2 + \ldots + c_\alpha \equiv c_{\alpha 1} j_1 + c_{\alpha 2} j_2 + \ldots + c_\alpha$$
$$(\alpha = 1, 2, \ldots, \varkappa)$$

nur durch $i_1 \equiv j_1, i_2 \equiv j_2, \ldots, i_\varkappa \equiv j_\varkappa$, oder daß für $i_1 - j_1 = z_1, i_2 - j_2 = z_2, \ldots$ die Kongruenzen

$$c_{\alpha 1} z_1 + c_{\alpha 2} z_2 + \ldots + c_{\alpha\varkappa} z_\varkappa \equiv 0$$
$$(\alpha = 1, 2, \ldots, \varkappa)$$

nur durch $z_1 \equiv z_2 \equiv \ldots \equiv z_\varkappa \equiv 0$ befriedigt werden. Dazu ist bekanntlich notwendig und hinreichend die Bedingung

(8) $$\Delta = |c_{\alpha\beta}| \text{ nicht } \equiv 0 \pmod p \qquad (\alpha, \beta = 1, 2, \ldots, \varkappa).$$

Die so bestimmten t bilden die lineare Gruppe; daß die Gruppeneigenschaften gewahrt sind, folgt leicht.

Aus (7) leiten wir durch rechtsseitige Multiplikation mit $s(-c)$ die Substitutionen

$$(9)\quad u = |\Sigma c_{1\beta} i_\beta,\ \Sigma c_{2\beta} i_\beta,\ \ldots,\ \Sigma c_{\varkappa\beta} i_\beta| \quad (\beta = 1, 2, \ldots, \varkappa)$$

her, die offenbar auch eine Gruppe bilden. Wir werden sie die lineare homogene Gruppe nennen und mit B bezeichnen.

§ 131. Wir wollen die Ordnung von B bestimmen, d. h. die Anzahl aller Substitutionen (9), für die (8) gilt. Sie sei durch $r_\varkappa$ bezeichnet, und es sei ferner $N_\varkappa$ die Anzahl der Substitutionen (9), für die

$$c_{11} \equiv 1,\ c_{12} \equiv c_{13} \equiv \ldots \equiv c_{1\varkappa} \equiv 0$$

ist, die also den ersten Index i_1 ungeändert lassen. Wir bezeichnen diese Substitutionen u durch $u_1', u_2', u_3', \ldots$ Wenn dann u eine beliebige andere Substitution (9) ist, so werden alle

$$(10)\qquad u_1' u,\ u_2' u,\ \ldots,\ u_N' u$$

den ersten Index i_1 in ein und derselben Weise umsetzen und nur sie auf diese Weise; nämlich so, daß der Index i_1 in einen bestimmten Wert

$$(11)\qquad c_{11} i_1 + c_{12} i_2 + \ldots + c_{1\varkappa} i_\varkappa$$

übergeht. Ordnet man die sämtlichen Substitutionen von B in solche Komplexe (10) ein, so sieht man, daß $r_\varkappa = N_\varkappa \cdot \varrho_\varkappa$ ist, wo $\varrho_\varkappa$ angibt, auf wieviel Arten die Koeffizienten $c_{1\alpha}$ in (11) wählbar sind. Da die einzige von ihnen zu erfüllende Bedingung die ist, daß nicht alle $c_{1\alpha}$ der Null kongruent werden, so ist $\varrho_\varkappa = p^\varkappa - 1$ und $r_\varkappa = (p^\varkappa - 1) N_\varkappa$.

Die u_α' haben die Gestalt

$$u' = |i_1,\ c_{21} i_1 + c_{22} i_2 + \ldots + c_{2\varkappa} i_\varkappa,\ \ldots,$$
$$\ldots,\ c_{\varkappa 1} i_1 + c_{\varkappa 2} i_2 + \ldots + c_{\varkappa\varkappa} i_\varkappa|.$$

Hier können die $c_{21}, c_{31}, \ldots, c_{\varkappa 1}$ völlig beliebig gewählt werden, da sie den Wert von Δ gar nicht beeinflussen; die Wahl kann also auf $p^{\varkappa-1}$ Arten geschehen. Die übrigen Koeffizienten in u' unterliegen dann nur der Bedingung, daß die Determinante

$$|c_{\alpha\beta}| \text{ nicht } \equiv 0 \pmod{p}, \qquad (\alpha, \beta = 2, 3, \ldots, \varkappa)$$

ist. Ihre Wahl kann daher nach der oben eingeführten Bezeichnung auf $r_{\varkappa-1}$ Arten geschehen. Demnach wird $N_\varkappa = p^{\varkappa-1} r_{\varkappa-1}$ und weiter

$$r_\varkappa = (p^\varkappa - 1) p^{\varkappa-1} r_{\varkappa-1} = (p^\varkappa - 1) p^{\varkappa-1} (p^{\varkappa-1} - p) p^{\varkappa-2} r_{\varkappa-2} = \ldots,$$

also

$$(12) \qquad r_\varkappa = (p^\varkappa - 1)(p^\varkappa - p)(p^\varkappa - p^2) \ldots (p^\varkappa - p^{\varkappa-1}) .$$

Das ist die gesuchte Ordnung von B. Sie ist durch die Primzahlpotenz $p^{\frac{1}{2}\varkappa(\varkappa-1)}$ teilbar. B hat also einen Teiler von der Ordnung $p^{\frac{1}{2}\varkappa(\varkappa-1)}$.

§ 132. Hat die Substitution u mit den Koeffizienten $c_{\alpha\beta}$ die Determinante $\varDelta = |c_{\alpha\beta}|$ und die Substitution u' mit den Koeffizienten $c'_{\alpha\beta}$ die Determinante $\varDelta' = |c'_{\alpha\beta}|$, dann hat bekanntlich die Substitution $u \cdot u'$ mit den Koeffizienten $\Sigma c_{\alpha\varrho} c'_{\varrho\beta}$ $(\varrho = 1, 2, \ldots, \varkappa)$ die Determinante $\varDelta \cdot \varDelta'$. Daraus folgt sofort, daß die Substitutionen u mit der Determinante 1 der Koeffizienten einen selbstkonjugierten Teiler von B bilden. Denn ist ω eine dieser Substitutionen, so ist die Determinante von $u^{-1} \omega u$ wieder gleich $\varDelta^{-1} \cdot \varDelta = 1$. Die Gruppe der ω werde durch Ω bezeichnet.

Jetzt sei e eine primitive Kongruenzwurzel modulo p, so daß die Reste des Komplexes

$$e^1, e^2, e^3, \ldots, e^{p-1} \pmod p$$

alle Zahlen $1, 2, 3, \ldots, p-1$ bis auf die Reihenfolge liefern.

$$u_0 = |e\, i_1, i_2, i_3, \ldots, i_\varkappa|$$

ist eine Substitution u aus B von der Determinante e, und der Komplex $u_0 \Omega$ umfaßt nach schon häufig verwendeten Schlüssen alle und nur die Substitutionen u, deren Determinante $\equiv e$ ist; ebenso $u_0^2 \Omega$ alle und nur die von der Determinante e^2, usw. Folglich hat man die Zerlegung von B in Komplexe

$$B = \Omega + u_0 \Omega + u_0^2 \Omega + \ldots + u_0^{p-2} \Omega .$$

Daraus ersieht man: die Ordnung von Ω ist gleich $r_\varkappa : (p-1)$; die Faktorgruppe B/Ω ist zyklisch und von der Ordnung $(p-1)$.

§ 133. Wir wollen versuchen, die Gruppe B aus mög-

lichst einfachen Substitutionen zusammenzusetzen. Dazu betrachten wir alle Substitutionen der Form

$$(13) \qquad \psi(\alpha/\beta) = |i_1, i_2, \ldots, i_{\alpha-1}, i_\alpha + i_\beta, i_{\alpha+1}, \ldots i_\varkappa| \quad (\alpha \neq \beta),$$

deren Anzahl gleich $\varkappa(\varkappa - 1)$ ist. $\psi(\alpha/\beta)$ gehört für jede Wahl von α und β zu B, ja zu Ω. Bezeichnen wir

$$c_{\sigma 1} i_1 + c_{\sigma 2} i_2 + c_{\sigma 3} i_3 + \ldots + c_{\sigma \varkappa} i_\varkappa = C_\sigma,$$

also die Substitutionen von B kurz durch

$$|C_1, C_2, C_3, \ldots, C_\varkappa|,$$

so wird

$$|C_1, C_2, C_3, \ldots, C_\varkappa| \cdot \psi(\alpha/\beta)$$
$$= |C_1, C_2, \ldots, C_{\alpha-1}, C_\alpha + C_\beta, C_{\alpha+1}, \ldots, C_\varkappa|,$$

d. h. die rechtsseitige Multiplikation einer Substitution aus B mit $\psi(\alpha/\beta)$ bewirkt die Addition des βten Index zum αten ohne weitere Änderungen der Indizes.

Nicht alle Koeffizienten von $i_\varkappa$ in $C_1, C_2, C_3, \ldots, C_\varkappa$ können verschwinden; denn sonst wäre, gegen (8), die Determinante $\Delta = 0$. Wir können die Bezeichnungen so wählen, daß $c_{\varkappa\varkappa} \neq 0$ ist. Dann bilden wir mit noch unbestimmten $y_1, y_2, \ldots, y_{\varkappa-1}$ als Exponenten die Komposition

$$|C_1, C_2, \ldots, C_\varkappa| \cdot \psi(1/\varkappa)^{y_1} \psi(2/\varkappa)^{y_2} \ldots \psi(\varkappa-1/\varkappa)^{y_\varkappa}$$
$$= |C_1 + y_1 C_\varkappa, C_2 + y_2 C_\varkappa, \ldots, C_{\varkappa-1} + y_{\varkappa-1} C_\varkappa, C_\varkappa|$$

und bestimmen die $y_1, y_2, \ldots, y_{\varkappa-1}$ so, daß im Resultate das $i_\varkappa$ der ersten $(\varkappa - 1)$ Indizes fortfällt. Das wird durch die Lösung von $(\varkappa - 1)$ linearen Kongruenzen erreicht, nämlich von

$$c_{1\varkappa} + y_1 c_{\varkappa\varkappa} \equiv 0, \quad c_{2\varkappa} + y_2 c_{\varkappa\varkappa} \equiv 0, \quad \ldots,$$
$$c_{\varkappa-1,\varkappa} + y_{\varkappa-1} c_{\varkappa\varkappa} \equiv 0.$$

In ähnlicher Art können wir aus den $(\varkappa - 2)$ ersten Indizes das $i_{\varkappa-1}$ entfernen, wofür möglicherweise die Aufeinanderfolge in den $(\varkappa - 1)$ ersten Indizes geändert werden muß. Weiter kann man aus den $(\varkappa - 3)$ ersten

Indizes auch das $i_{\varkappa-2}$ eliminieren usf., bis wir auf eine Substitution der Form

$$|c_{11} i_1, c_{21} i_1 + c_{22} i_2, c_{31} i_1 + c_{32} i_2 + c_{33} i_3, \ldots, \\ \ldots, c_{\varkappa 1} i_1 + c_{\varkappa 2} i_2 + \ldots + c_{\varkappa\varkappa} i_\varkappa|$$

mit c_{11} nicht $\equiv 0$ kommen. Aus dieser führt uns die weitere rechtsseitige Multiplikation mit

$$\psi(2/1)^{y_2} \psi(3/1)^{y_3} \ldots \psi(\varkappa/1)^{y_\varkappa}$$

bei passend gewählten Exponenten y auf eine Substitution der Form

$$|c_{11} i_1, c_{22} i_2, c_{32} i_2 + c_{33} i_3, \ldots, c_{\varkappa 2} i_2 + \ldots + c_{\varkappa\varkappa} i_\varkappa| \\ (c_{22} \text{ nicht } \equiv 0)$$

und so fort, bis man zu einem „Diagonalsystem" oder einer „Multiplikation"

(14) $$|c_{11} i_1, c_{22} i_2, \ldots, c_{\varkappa\varkappa} i_\varkappa|$$

gelangt, wie eine Substitution von der Form (14) heißen soll.

Weil nun die Reziproke von ψ, nämlich

$$\psi(\alpha/\beta)^{-1} = |i_1, i_2, \ldots, i_\alpha - i_\beta, \ldots, i_\varkappa|,$$

auch von der Form der ψ ist, so folgt, daß jede Substitution von B gleich einem Produkte

(15) $$\prod_{\alpha, \beta} \psi(\alpha/\beta) \cdot |c_{11} i_1, c_{22} i_2, \ldots, c_{\varkappa\varkappa} i_\varkappa|$$

gesetzt werden kann.

Da ferner jedes ψ die Determinante 1 hat, so ist die Bedingung dafür, daß (15) eine Substitution von Ω wird, in der Kongruenz enthalten

(16) $$c_{11} c_{22} \ldots c_{\varkappa\varkappa} \equiv 1 \pmod{p}.$$

Wir bemerken noch, daß die Reziproke des Diagonalsystems (14) gleich

(14*) $$\left|\frac{1}{c_{11}} i_1, \frac{1}{c_{22}} i_2, \ldots, \frac{1}{c_{\varkappa\varkappa}} i_\varkappa\right|,$$

also auch ein Diagonalsystem wird.

Zu weiteren Reduktionen führt uns eine Kombination aus vier ψ-Funktionen. Wir setzen, wenn α nicht $\equiv 0 \bmod p$,

$$\chi\left(1/2\,;\,\frac{1}{\alpha}\right) = \psi(1/2)^{\alpha-1}\,\psi(2/1)\,\psi(1/2)^{\frac{1}{\alpha}-1}\,\psi(2/1)^{-\alpha}\,,$$

wobei $\frac{1}{\alpha}$ die ganze Zahl z bedeutet, die der Kongruenz

$$\alpha z \equiv 1 \pmod p$$

genügt; eine solche besteht, denn α soll nicht $\equiv 0 \pmod p$ sein. Es wird dann der Wert der rechten Seite

$$\begin{aligned}\chi\left(1/2\,;\,\frac{1}{\alpha}\right) &= |i_1 + (\alpha-1)\,i_2\,,\; i_2\,,\; \ldots| \cdot |i_1\,,\; i_2 + i_1\,,\; i_3\,,\; \ldots| \\ &\quad \cdot \left|i_1 + \left(\frac{1}{\alpha} - 1\right) i_2\,,\; i_2\,,\; \ldots\right| \cdot |i_1\,,\; i_2 - \alpha\, i_1\,,\; i_3\,,\; \ldots| \\ &= |i_1 + (\alpha-1)\,i_2\,,\; i_1 + \alpha\, i_2\,,\; i_3\,,\; \ldots| \\ &\quad \cdot \left|i_1 + \left(\frac{1}{\alpha} - 1\right) i_2\,,\; \alpha(-i_1 + i_2)\,,\; \ldots\right| \\ &= \left|\frac{1}{\alpha}\, i_1\,,\; \alpha\, i_2\,,\; i_3\,,\; \ldots,\; i_\varkappa\right|\,;\end{aligned}$$

und weiter ergibt sich unter Benutzung dieses Resultates

$$\begin{aligned}&|c_{11}\, i_1\,,\; c_{22}\, i_2\,,\; \ldots,\; c_{\varkappa\varkappa}\, i_\varkappa| \\ &= |c_{11}\, c_{22}\, i_1\,,\; i_2\,,\; c_{33}\, i_3\,,\; \ldots,\; c_{\varkappa\varkappa}\, i_\varkappa|\, \chi(1/2\,;\, c_{22}) \\ &= |c_{11}\, c_{22}\, c_{33}\, i_1\,,\; i_2\,,\; i_3\,,\; c_{44}\, i_4\,,\; \ldots|\, \chi(1/3\,;\, c_{33})\, \chi(1/2\,;\, c_{22}) = \ldots \\ &= |\Pi c_{\alpha\alpha}\, i_1\,,\; i_2\,,\; \ldots,\; i_\varkappa| \cdot \Pi \chi(1/\beta\,;\, c_{\beta\beta})\,,\end{aligned}$$

und ebenso

$$= \Pi \chi(1/\beta\,;\, c_{\beta\beta}) \cdot |(c_{11} \ldots c_{\varkappa\varkappa})\, i_1\,,\; i_2\,,\; \ldots,\; i_\varkappa|\,.$$

Unter Berücksichtigung von (15) erkennt man, daß jede Substitution von B mit der Determinante d gleich einem Produkte

$$\Pi \psi(\alpha/\beta) \cdot |d\, i_1\,,\; i_2\,,\; \ldots,\; i_\varkappa|\,,$$

also jede von Ω gleich einem Produkte

$$\Pi \psi(\alpha/\beta)$$

gesetzt werden kann. Es sind noch weitere Reduktionen der $\psi(\alpha/\beta)$ möglich, derart, daß nur Funktionen $\psi(1/\beta)$ oder $\psi(\alpha/1)$ auftreten; doch wollen wir hierauf nicht weiter eingehen.

§ 134. Abgesehen von dem Vorzuge der Einfachheit ihrer Bildung haben die besprochenen Gruppen linearer Substitutionen noch eine besonders hervorragende Bedeutung. Das geht aus den folgenden Untersuchungen hervor und steht in Beziehung zur Theorie der auflösbaren Gruppen.

Wir wollen die transitiven auflösbaren Gruppen des Primzahlgrades p untersuchen. G sei eine solche Substitutionengruppe; ihr Grad sei p; ihre Elemente $x_0, x_1, \ldots, x_{p-1}$. Ihre Ordnung r ist als Teiler von $p!$ und als Vielfaches von p durch p^1, aber durch keine höhere Potenz von p teilbar. Die letzte Gruppe der Hauptreihe von G, unmittelbar vor der Einheit sei M. Dann ist M als selbstkonjugierter Teiler der primitiven Gruppe G transitiv in den Elementen $x_0, x_1, x_2, \ldots, x_{p-1}$ nach § 114, S. 145; die Ordnung von M ist daher ein Vielfaches von p und nach § 58, S. 75 eine Potenz von p. Nach den obigen Darlegungen kann es nur p^1 sein. Die letzte Gruppe der Hauptreihe von G vor der Einheit ist eine zyklische Gruppe des Grades und der Ordnung p; sie ist von der Form

$$M = \{(x_0 x_1 \ldots x_{p-1})\} = \{|x_z, x_{z+1}|\} = |z, z+1| \pmod{p}.$$

Zu den voraufgehenden Gliedern der Kompositionsreihe von G führen die Untersuchungen aus § 103, S. 132. Diesen zufolge gehören sämtliche Substitutionen, die M in sich selbst transformieren, zur metazyklischen Gruppe der Ordnung $p(p-1)$, d. h. die auflösbaren transitiven Gruppen des Primzahlgrades p sind Teiler der metazyklischen, daher auch der linearen Gruppe gleichen Grades.

Der gewonnene Satz läßt sich umkehren: Die metazyklische Gruppe des Primzahlgrades p ist auflösbar.

Diese Gruppe G kann nämlich nach unseren Untersuchungen (§ 103, S. 132) folgendermaßen dargestellt werden: es sei a eine primitive Kongruenzwurzel modulo p, und

$$s = |z+1|, \quad t = |az| \pmod{p},$$

wobei z den Index der Elemente $x_0, x_1, \ldots, x_{p-1}$ allgemein darstellt. Dann ist

$$G = \{s, t\}.$$

Um die Konstitution von G zu ergründen, zerlegen wir $(p-1)$ in seine Primfaktoren

$$p - 1 = q_1 q_2 q_3 \cdots q_\varrho$$

und setzen, die q in willkürlicher Folge genommen,

$$a^{q_1} = a_1, \quad a_1^{q_2} = a_2, \quad \ldots, \quad a_{\varrho-1}^{q_\varrho} = a_\varrho;$$

$$t_1 = |a_1 z|, \quad t_2 = |a_2 z|, \quad \ldots, \quad t_\varrho = |a_\varrho z| = |z|;$$

dann ist

$$G = \{s, t\}, \quad G_1 = \{s, t_1\}, \quad G_2 = \{s, t_2\}, \quad \ldots,$$
$$G_\varrho = \{s, t_\varrho\} = \{s\}, \quad 1$$

eine der Kompositionsreihen von G; die zugehörigen Zahlfaktoren der Komposition sind hier die Primzahlen

$$q_1, q_2, q_3, \ldots, q_\varrho, p;$$

also ist G auflösbar.

§ 135. Die gewonnenen Resultate lassen sich noch verallgemeinern.

Es sei G eine primitive auflösbare Gruppe des Grades p^α. In der Hauptreihe von G möge M das Glied sein, das unmittelbar vor der Einheit steht. Nach § 114, S. 145 ist M transitiv in den p^α Elementen von G und nach dem Schlußsatze jenes Paragraphen eine Abelsche Gruppe des Typus $(1, 1, 1, \ldots, 1)$. Nach § 108, S. 141 ist ihr Grad gleich ihrer Ordnung; also hat M die Ordnung p^α, und das Symbol $(1, 1, 1, \ldots, 1)$ umfaßt α Einheiten. Die Substitutionengruppe M ist einstufig isomorph in der Form

$$b_1^{\lambda_1} b_2^{\lambda_2} \ldots b_\alpha^{\lambda_\alpha} \qquad (\lambda = 0, 1, 2, \ldots, p-1)$$

darstellbar, wenn die b voneinander unabhängige und miteinander vertauschbare Operatoren der Ordnung p bedeuten. Um diese Darstellung analytisch zu gestalten, setzen wir

$$b_1^{\lambda_1} b_2^{\lambda_2} \ldots b_\alpha^{\lambda_\alpha} = x_{\lambda_1, \lambda_2, \ldots, \lambda_\alpha} \qquad (\lambda = 0, 1, 2, \ldots, p-1),$$

erkennen sofort, daß die Gleichung

$$x_{\lambda_1, \lambda_2, \ldots} \cdot x_{\mu_1, \mu_2, \ldots} = x_{\lambda_1+\mu_1, \lambda_2+\mu_2, \ldots}$$

besteht, und schließen daraus, daß M aus den α einfachen Substitutionen

$$s_1 = |i_1 + 1, i_2, \ldots, i_\alpha|, \quad s_2 = |i_1, i_2 + 1, \ldots, i_\alpha|, \quad \ldots, \quad s_\alpha = |i_1, i_2, \ldots, i_\alpha + 1|$$

hervorgeht und mit der arithmetischen Gruppe identisch ist. Die letzte Gruppe der Hauptreihe einer primitiven auflösbaren Gruppe des Grades p^α besteht aus den p^α arithmetischen Substitutionen der Elemente $x_{z_1, z_2, \ldots, z_\alpha}$

$$|z_1 + \beta_1, z_2 + \beta_2, \ldots, z_\alpha + \beta_\alpha|$$
$$(\beta = 0, 1, 2, \ldots, p - 1; \quad (\mathrm{mod}\, p)) .$$

Jetzt ermöglichen uns die in § 130, S. 166 erlangten Resultate, einen Schritt weiter zu gehen. Es hat sich nämlich dort gezeigt, daß die einzigen Substitutionen, die M in sich selbst transformieren, der linearen Gruppe des Grades p^α angehören. Eine primitive Gruppe vom Grade p^α kann nur auflösbar sein, wenn sie ein Teiler der linearen Gruppe dieses Grades ist (E. Galois). Die Umkehrung dieses Satzes ist nicht allgemein gültig; die Bestimmung aller auflösbaren Teiler der linearen Gruppe führt auf schwierige Probleme.

Namen- und Sachregister.

(Die Zahlen geben die Seiten an.)

Abelsche Gruppen 52, 82 ff., 99,
Abstrakte Gruppen 15. [141,
Alternierende Gruppen 14, 81,
127, 148.
Arithmetische Gruppen 165.
Auflösbare Gruppen 115 ff., 149,
[173, 174.

Bochert 129.
Burnside 122, 146.

Cauchy 98, 105.
Cayley 21.

Dedekind 95, 98.
Diagonalsystem 171.
Direktes Produkt 59.
Divisor 35.

Einfache Gruppen 55.
Einheitsoperator 17.
Einstufiger Isomorphismus 40.
Elemente 5.
Endliche Gruppen 4.

Faktor linksseitig, rechtsseitig 2.
Faktorgruppe 60.
Frobenius 99 ff., 117 ff.

Galois 116, 175.
Grad von Substitutionengruppen
[8.

Hamiltonsche Gruppen 95.
Hauptreihe 71.
Hurwitz 15.

Imprimitive Gruppen 142 ff.
Index 36, 38, 156.
Intransitive Gruppen 124, 139.
Invarianten Abelscher Gruppen
Inversion 11. [87.
Isomorphismus 40, 150.

Jordan 117, 146.

Klassen von Substitutionen 11,
Komplex, Komplexion 2. [12.
Komponente 2.
Kompositionsfaktor 68.
Kompositionsreihe 67.
Konjugierte Teiler 55.
Konstitution 42.
Kronecker 133.

Lineare Gruppe 168, 175.

Maximalteiler 65.
Mehrstufiger Isomorphismus 40.
Metazyklische Gruppen 133, 173.
Multiplikation 2, 35, 171.

Nebenkomplexe 36.

Operator 2.
Ordnung einer Gruppe 4.
Ordnung eines Operators 17.
Ordnung einer Substitution 10.

Permutation 5.
Potenz eines Operators 16.
Primitive Gruppen 143 ff.
Produkt 2, 6.
Produkt, direktes 59.

Quadrat, Cayleysches 21 ff.
Quadrat, lateinisches 22.
Quaternionengruppe 95.

Rang Abelscher Gruppen 87.
Reguläre Gruppen 28, 147.
Reziproke 7, 17.

Selbstkonjugierter Operator 56.
Selbstkonjugierter Teiler 55.
Substitution 5.
Substitution, ähnliche 48.
Substitutionengruppe 8.
Sylow 99 ff., 120.
Symmetrische Gruppen 7, 127,
[148.

Teiler 35.
Transformation 47.
Transformationskomplex 55.
Transitivität 123 ff.

Unendliche Gruppen 4, 32.
Untergruppen 35.

Vertauschbare Gruppen 52.
Vertauschbare Operatoren 50, 52.

Zahlfaktoren der Hauptreihe 72.
Zahlfaktoren der Kompositionsreihe 68.
Zusammengesetzte Gruppen 55 ff.
Zusammensetzungsreihe 67.
Zwischengruppe 54.
Zykel 8.
Zyklische Gruppen 30.

G. J. Göschen'sche Verlagshandlung in Leipzig.

1.

it
0.
r
-,

n.
0.
n-
lt
re
e-
is
r-

nd
e.
it
s-
rd
er

n-
nd
ng
en
nd
in
en.